(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－92721
（P2001－92721A）
(43)公開日　平成13年４月６日(2001.4.6)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
G06F	12/14	320	G06F	12/14	320F　5B017
	13/00	354		13/00	354D　5B049
	17/60			15/21	330　5B089
G10L	11/00		G10L	9/00	E　9A001

審査請求　未請求　請求項の数８　ＯＬ　（全 38 頁）

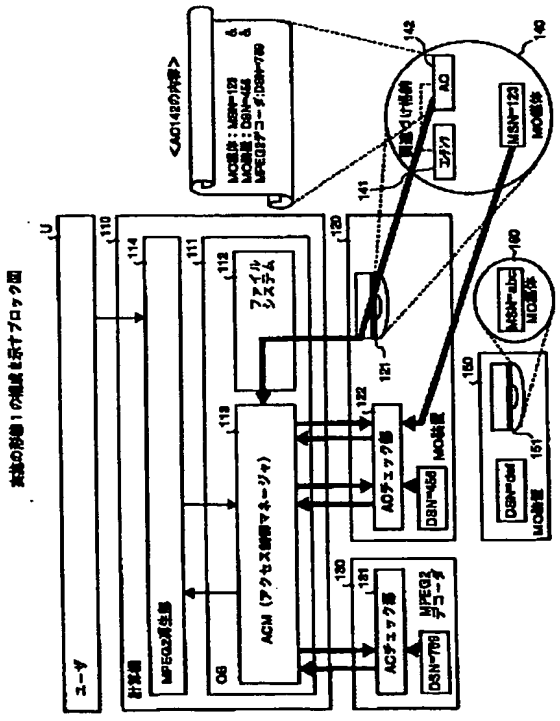
(21)出願番号　特願平11－264616
(22)出願日　平成11年９月17日(1999.9.17)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　蒲田　順
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100089118
弁理士　酒井　宏明

最終頁に続く

(54)【発明の名称】　コンテンツ利用制御装置、コンテンツ利用制御システムおよびコンテンツ利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　コンテンツを容易に利用することができるとともに、コンテンツの不正利用を防止すること。
【解決手段】　コンテンツ１４１を利用するためのものであって、それぞれに識別情報（ＭＳＮ＝１２３、ＤＳＮ＝４５６、ＤＳＮ＝７８９）が付与されたＭＯ装置１２０、ＭＰＥＧ２デコーダ１３０およびＭＯ媒体１４０を備え、このＭＯ媒体１４０には、コンテンツ１４１に関連づけられたＡＣ（許諾情報）１４２が記録されており、ＡＣ１４２および識別情報に基づいて、コンテンツ１４１の利用が制御される。



【特許請求の範囲】

【請求項１】　情報提供権限者から利用者に提供されるコンテンツの利用制御を行うコンテンツ利用制御装置において、

前記コンテンツが記録されたメディアを含み、前記コンテンツを利用するための利用手段であって、自身を構成する物理要素に関する識別情報が付与された利用手段と、

前記利用手段に付与された識別情報および前記コンテンツの利用に関する許諾情報に基づいて、前記コンテンツの利用を制御する利用制御手段とを備え、

前記メディアには、前記コンテンツに関連づけられた前記許諾情報が記録されていることを特徴とするコンテンツ利用制御装置。

【請求項２】　前記許諾情報は、複数の物理要素に対応する複数の部分許諾情報からなり、前記メディアには、前記複数の物理要素に対応するそれぞれの識別情報で多重暗号化された前記複数の部分許諾情報が記録されており、前記利用制御手段は、前記複数の物理要素に対応するそれぞれの識別情報と、前記複数の物理要素に対応するそれぞれの識別情報を用いて前記部分許諾情報を復号した結果とに基づいて、前記コンテンツの利用を制御することを特徴とする請求項１に記載のコンテンツ利用制御装置。

【請求項３】　前記メディアには、暗号化されたコンテンツが記録されているとともに、前記複数の部分許諾情報および前記コンテンツを復号するためのコンテンツ復号鍵が多重暗号化されたものが記録されており、前記利用手段は、前記利用制御手段により利用が許諾された場合に、前記コンテンツ復号鍵を用いて前記コンテンツを復号した結果に基づいてコンテンツを利用することを特徴とする請求項２に記載のコンテンツ利用制御装置。

【請求項４】　前記メディアは、暗号化された情報が記録されるセキュア領域を有しており、前記セキュア領域には、暗号化された前記許諾情報が記録されており、前記利用制御手段は、前記セキュア領域に記録された前記許諾情報の復号結果および前記識別情報に基づいて、前記コンテンツの利用を制御することを特徴とする請求項１に記載のコンテンツ利用制御装置。

【請求項５】　前記利用手段は、少なくとも二つの物理要素で構成され、前記二つの物理要素は、相互認証コマンドが発行された際に相互認証を行い、前記メディアは、前記相互認証コマンドが発行されかつ前記相互認証がとられた場合にのみアクセス可能な特別領域を有しており、前記特別領域には、前記許諾情報が格納されており、前記利用制御手段は、前記相互認証コマンドが発行されかつ前記相互認証がとられた場合にのみ、前記特別領域から前記許諾情報を取得し、該許諾情報および前記識別情報に基づいて、前記コンテンツの利用を制御することを特徴とする請求項１に記載のコンテンツ利用制御装置。

【請求項６】　前記特別領域は、暗号化された情報が記録されるセキュア領域とマッピングされていることを特徴とする請求項５に記載のコンテンツ利用制御装置。

【請求項７】　情報提供権限者から利用者に提供されるコンテンツと、前記コンテンツの利用に関する許諾情報とが関連付けられて記録されたメディアから、前記コンテンツおよび前記許諾情報を読み出す読出手段と、

読み出された前記コンテンツと前記許諾情報とを一つのファイルとして転送する転送手段と、

前記一つのファイルを受信する受信手段と、

前記受信手段により受信された前記一つのファイルから前記コンテンツおよび前記許諾情報を生成し、これらを別のメディアに書き込む書込手段とを備えることを特徴とするコンテンツ利用制御システム。

【請求項８】　情報提供権限者から利用者に提供されるコンテンツが記録されたメディアを含み、前記コンテンツを利用するための利用手段であって、自身を構成する物理要素に関する識別情報が付与された利用手段を備えるコンテンツ利用制御装置に適用されるコンテンツ利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記メディアには、前記コンテンツに関連づけられた前記許諾情報が記録されており、

前記利用手段に付与された識別情報および前記コンテンツの利用に関する許諾情報に基づいて、前記コンテンツの利用を制御させる利用制御工程をコンピュータに実行させるための利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、著作権者等の情報提供権限者により提供されるコンテンツの利用に関する制御を行うコンテンツ利用制御装置、コンテンツ利用制御システムおよびコンテンツ利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体に関するものである。

【０００２】近時においては、ディジタル化された映画、音楽等のコンテンツの配信が本格的にスタートしたことから、この種のコンテンツに関する著作権、許諾を管理する機構の実現が急がれている。

【０００３】

【従来の技術】従来より、映画、音楽等のコンテンツ（著作物）に関しては、著作者の許諾を得なければ、営利目的で販売、譲渡することができない。ここでいうコンテンツは、単一の記録媒体に記録可能なビット列の集合としての構造をもつディジタルコンテンツであり、文章テキスト、静止画、動画、プログラムソフトウェア等をいう。

【０００４】この種のコンテンツは、記録媒体に記録さ

れた状態で利用者に配布される。この場合、著作権保護を目的として、許諾情報を用いたコンテンツの利用に関する制御（以下、コンテンツ利用制御という）が行われる。このコンテンツ利用制御は、正当な許諾を受けた利用者のみがコンテンツを利用できるようにするためのものである。

【０００５】たとえば、コンテンツ利用制御の一例としては、コンテンツを利用する上で必要な物理要素（システム（記録媒体、装置））を特定するための識別情報からなる許諾情報を利用するものがある。この許諾情報には、コンテンツの利用に関する許諾条件が含まれている。上記システムには、固有の識別情報が付与されている。この場合、利用者は、コンテンツの入手経路とは別の経路から上記許諾情報を入手する。つぎに、利用者は、上記許諾情報をシステムに入力した後、このシステムにコンテンツが記録された記録媒体をセットする。

【０００６】これにより、システムは、自身に付与されている識別情報が、利用者により入力された許諾情報に含まれる許諾条件を満たしているか否かを判断する。ここで、許諾条件を満たしている場合には、コンテンツの利用が許諾される。一方、許諾条件を満たしていない場合には、コンテンツの利用が許諾されない。

【０００７】

【発明が解決しようとする課題】ところで、前述したように、従来においては、コンテンツを利用する場合、コンテンツが記録された記録媒体と、許諾情報とを別々の経路から入手しなければならないため、非常に不便である。また、従来においては、記録媒体と許諾情報とが別になっているため、一方を紛失する可能性がある。

【０００８】さらに、従来においては、許諾情報のみが単体で存在しているため、許諾情報の不正コピーが可能であり、この結果、コンテンツが不正利用されるという問題があった。これは、著作権者保護の観点から許容されるものではない。

【０００９】本発明は、上記に鑑みてなされたもので、コンテンツを容易に利用することができ、コンテンツの不正利用を防止することができるコンテンツ利用制御装置、コンテンツ利用制御システムおよびコンテンツ利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【００１０】上記目的を達成するために、請求項１にかかる発明は、情報提供権限者から利用者に提供されるコンテンツの利用制御を行うコンテンツ利用制御装置において、前記コンテンツが記録されたメディア（後述する実施の形態１のMO媒体１４０に相当）を含み、前記コンテンツを利用するための利用手段であって、自身を構成する物理要素に関する識別情報が付与された利用手段（後述する実施の形態１のMO装置１２０、ＭＰＥＧ２デコーダ１３０、MO媒体１４０に相当）と、前記利用手段に付与された識別情報および前記コンテンツの利用に関する許諾情報に基づいて、前記コンテンツの利用を制御する利用制御手段（後述する実施の形態１の計算機１１０に相当）とを備え、前記メディアには、前記コンテンツに関連づけられた前記許諾情報が記録されていることを特徴とする。

【００１１】この請求項１にかかる発明によれば、利用制御手段は、メディアから取得した許諾情報と識別情報とに基づいて、コンテンツの利用を制御する。ここで、利用が許諾された場合には、利用手段は、メディアからコンテンツを取得した後、これを利用する。

【００１２】このように、請求項１にかかる発明によれば、許諾情報とコンテンツとを関連付けて一つのメディアに記録し、この許諾情報および識別情報に基づいて、コンテンツの利用の制御を行うようにしたので、一つのメディアを入手することで同時に許諾情報とコンテンツとが得られるため、許諾情報とコンテンツとを別々に入手していた従来に比して、コンテンツを容易に利用することができる。

【００１３】また、請求項２にかかる発明は、請求項１に記載のコンテンツ利用制御装置において、前記許諾情報は、複数の物理要素に対応する複数の部分許諾情報からなり、前記メディア（後述する実施の形態２のMO媒体２４０に相当）には、前記複数の物理要素に対応するそれぞれの識別情報で多重暗号化された前記複数の部分許諾情報が記録されており、前記利用制御手段（後述する実施の形態２の計算機２１０に相当）は、前記複数の物理要素に対応するそれぞれの識別情報と、前記複数の物理要素に対応するそれぞれの識別情報を用いて、前記部分許諾情報を復号した結果とに基づいて、前記コンテンツの利用を制御することを特徴とする。

【００１４】この請求項２にかかる発明によれば、利用制御手段は、メディアから取得した部分許諾情報を復号し、この復号結果と識別情報とに基づいて、コンテンツの利用を制御する。ここで、部分許諾情報をすべて復号できるのは、正当な許諾を受ける権限を有する利用者に属する装置である。したがって、部分許諾情報を復号できなかった場合には、当該装置は、不正利用者に属していることになる。

【００１５】このように請求項２にかかる発明によれば、複数の部分許諾情報を多重暗号化してメディアに記録するようにしたので、コンテンツの不正利用を防止することができる。

【００１６】また、請求項３にかかる発明は、請求項２に記載のコンテンツ利用制御装置において、前記メディア（後述する実施の形態３のMO媒体２４０に相当）には、暗号化されたコンテンツが記録されているとともに、前記複数の部分許諾情報および前記コンテンツを復号するためのコンテンツ復号鍵が多重暗号化されたものが記録されており、前記利用手段は、前記利用制御手段により利用が許諾された場合に、前記コンテンツ復号鍵

を用いて前記コンテンツを復号した結果に基づいてコンテンツを利用することを特徴とする。

【００１７】この請求項３にかかる発明によれば、利用制御手段は、メディアから取得した部分許諾情報を復号し、この復号結果と識別情報とに基づいて、コンテンツの利用を制御する。ここで、部分許諾情報およびコンテンツ復号鍵をすべて復号できるのは、正当な許諾を受ける権限を有する利用者に属する装置である。さらに、利用手段は、利用制御手段により利用が許諾された場合に、コンテンツ復号鍵を用いてコンテンツを復号した結果に基づいてコンテンツを利用する。

【００１８】このように請求項３にかかる発明によれば、複数の部分許諾情報に加えてコンテンツを復号するためのコンテンツ復号鍵を多重暗号化してメディアに記録するようにしたので、コンテンツの不正利用をより効果的に防止することができる。

【００１９】また、請求項４にかかる発明は、請求項１に記載のコンテンツ利用制御装置において、前記メディア（後述する実施の形態４のMO媒体４４０に相当）は、暗号化された情報が記録されるセキュア領域を有しており、前記セキュア領域には、暗号化された前記許諾情報が記録されており、前記利用制御手段は、前記セキュア領域に記録された前記許諾情報の復号結果および前記識別情報に基づいて、前記コンテンツの利用を制御することを特徴とする。

【００２０】この請求項４にかかる発明によれば、利用制御手段は、セキュア領域に記録された許諾情報の復号結果および識別情報に基づいて、コンテンツの利用を制御する。ここで、許諾情報を復号できるのは、正当な許諾を受ける権限を有する利用者に属する装置である。したがって、許諾情報を復号できなかった場合には、当該装置は、不正利用者に属していることになる。

【００２１】このように請求項４にかかる発明によれば、メディアのセキュア領域に暗号化された許諾情報を記録するようにしたので、コンテンツの不正利用を防止することができる。

【００２２】また、請求項５にかかる発明は、請求項１に記載のコンテンツ利用制御装置において、前記利用手段（後述する実施の形態５のファイルシステム５１０およびMO装置５２０に相当）は、少なくとも二つの物理要素で構成され、前記二つの物理要素は、相互認証コマンドが発行された際に相互認証を行い、前記メディア（後述する実施の形態５の５４０に相当）は、前記相互認証コマンドが発行されかつ前記相互認証がとられた場合にのみアクセス可能な特別領域を有しており、前記特別領域には、前記許諾情報が格納されており、前記利用制御手段は、前記相互認証コマンドが発行されかつ前記相互認証がとられた場合にのみ、前記特別領域から前記許諾情報を取得し、該許諾情報および前記識別情報に基づいて、前記コンテンツの利用を制御することを特徴とする。

【００２３】この請求項５にかかる発明によれば、相互認証コマンドが発行されると、二つの物理要素は、相互認証を行う。ここで、相互認証がとられた場合には、利用制御手段は、特別領域から許諾情報を取得し、該許諾情報および識別情報に基づいて、コンテンツの利用を制御する。一方、相互認証がとられなかった場合には、許諾が与えられない。

【００２４】このように、請求項５にかかる発明によれば、メディアの特別領域に許諾情報を記録し、二つの物理要素間で相互認証がとられた場合にのみ、該特別領域から許諾情報を取得するようにしたので、相互認証がとられない場合に、即時に許諾不可とすることができ、コンテンツの不正利用を防止することができる。

【００２５】また、請求項６にかかる発明は、請求項５に記載のコンテンツ利用制御装置において、前記特別領域（後述する実施の形態６の特別領域B_2 に相当）は、暗号化された情報が記録されるセキュア領域とマッピングされていることを特徴とする。

【００２６】この請求項６にかかる発明によれば、いずれもセキュリティ上有効である特別領域にセキュア領域をマッピングするようにしたので、極めて高いセキュリティを確保することができる。

【００２７】また、請求項７にかかる発明は、情報提供権限者から利用者に提供されるコンテンツと、前記コンテンツの利用に関する許諾情報とが関連付けられて記録されたメディアから、前記コンテンツおよび前記許諾情報を読み出す読出手段（後述する実施の形態７のファイルシステム８２２に相当）と、読み出された前記コンテンツと前記許諾情報とを一つのファイルとして転送する転送手段（後述する実施の形態７の転送部８２４に相当）と、前記一つのファイルを受信する受信手段（後述する実施の形態７の受信部９２４に相当）と、前記受信手段により受信された前記一つのファイルから前記コンテンツおよび前記許諾情報を生成し、これらを別のメディアに書き込む書込手段（後述する実施の形態７のファイルシステム９２２に相当）とを備えることを特徴とする。

【００２８】この請求項７にかかる発明によれば、読出手段によりメディアからコンテンツおよび許諾情報が読み出されると、転送手段によりコンテンツおよび許諾情報が一つのファイルとして転送される。そして、受信手段により、上記一つのファイルからコンテンツおよび許諾情報が生成される。書込手段は、コンテンツおよび許諾情報を別のメディアに書き込む。

【００２９】このように、請求項７にかかる発明によれば、一方のメディアから他方のメディアへコンテンツおよび許諾情報が転送（コピー）されるので、コンテンツの利用に関する許諾（ライセンス）を第三者に譲渡することができる。

【００３０】また、請求項８にかかる発明は、情報提供権限者から利用者に提供されるコンテンツが記録されたメディアを含み、前記コンテンツを利用するための利用手段であって、自身を構成する物理要素に関する識別情報が付与された利用手段を備えるコンテンツ利用制御装置に適用されるコンテンツ利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記メディアには、前記コンテンツに関連づけられた前記許諾情報が記録されており、前記利用手段に付与された識別情報および前記コンテンツの利用に関する許諾情報に基づいて、前記コンテンツの利用を制御させる利用制御工程（後述する実施の形態１のステップＳＡ１～ステップＳＡ１８に相当）をコンピュータに実行させるための利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００３１】この請求項８にかかる発明によれば、利用制御工程では、メディアから取得した許諾情報と識別情報とに基づいて、コンテンツの利用が制御される。ここで、利用が許諾された場合には、利用手段は、メディアからコンテンツを取得した後、これを利用する。

【００３２】このように、請求項８にかかる発明によれば、許諾情報とコンテンツとを関連付けて一つのメディアに記録し、これらの許諾情報および識別情報に基づいて、コンテンツの利用の制御を行うようにしたので、一つのメディアを入手することで同時に許諾情報とコンテンツとが得られるため、許諾情報とコンテンツとを別々に入手していた従来に比して、コンテンツを容易に利用することができる。

【００３３】

【発明の実施の形態】以下、図面を参照して本発明にかかるコンテンツ利用制御装置、コンテンツ利用制御システムおよびコンテンツ利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体の実施の形態１～８について詳細に説明する。

【００３４】（実施の形態１）図１は、本発明にかかる実施の形態１の構成を示すブロック図である。この図において、計算機１１０は、ユーザUにより操作されるものであり、ＯＳ（Oparating System）１１１を備えている。この計算機１１０においては、ＯＳ１１１により各種プログラムの実行が制御される。ファイルシステム１１２は、計算機１１０で扱われるファイルを管理し、データのリード／ライトを制御する。ＡＣＭ（Access Control Manager:アクセス制御マネージャ）１１３は、ファイルシステム１１２、ＭＰＥＧ２（Moving Picture Experts Group 2）再生部１１４、MO（Magneto Optic）装置１２０、ＭＰＥＧ２デコーダ１３０相互間のアクセス制御を管理する。

【００３５】ＭＰＥＧ２再生部１１４は、後述するＭＰＥＧ２デコーダ１３０へ動画データ（コンテンツ）を供給する等の制御を行う。実際には、ＭＰＥＧ２再生部１１４の機能は、ＭＰＥＧ２再生アプリケーションプログラム（図示略）が実行されることにより実現される。ＭＯ装置１２０は、計算機１１０に外付け（または内蔵）されており、MO媒体（同図の場合、MO媒体１４０）からデータを読み取る。

【００３６】このMO媒体１４０には、コンテンツ１４１とＡＣ（Access Condition：アクセス許可条件を示す情報）１４２とが関連付けられた状態で格納されている。このコンテンツ１４１は、たとえば、ＭＰＥＧ２方式の動画データであり、著作権者等の情報提供権限者により提供される。なお、コンテンツ１４１としては、著作権、許諾に関わるものであればそのデータ形式は問わない。ＡＣ１４２は、コンテンツ１４１の再生に関する許諾情報である。つまり、ＡＣ１４２の条件を満たす場合には、コンテンツ１４１の再生が許諾され、一方、ＡＣ１４２の条件を満たさない場合には、コンテンツ１４１の再生が許諾されない。

【００３７】ここで、ＡＣ１４２の条件は、複数の対象物理要素にそれぞれ付与された識別情報の組み合わせからなる。この対象物理要素としては、コンテンツ１４１を再生するために必要な装置、媒体であり、MO媒体、MO装置、ＭＰＥＧ２装置である。また、識別情報としては、ＭＳＮ（Media Serial Number：媒体シリアル番号）、ＤＳＮ（Device Serial Number：装置シリアル番号）である。具体的には、ＡＣ１４２においては、MO媒体のＭＳＮが「１２３」、MO装置のＤＳＮが「４５６」、ＭＰＥＧ２デコーダのＤＳＮが「７８９」に設定されている。また、ＡＣ１４２においては、ＭＳＮ（＝１２３）&ＤＳＮ（＝４５６）&ＤＳＮ（＝７８９）という論理積（アンド）条件が設定されている。

【００３８】つまり、ＡＣ１４２によれば、ＭＳＮ（＝１２３）が付与されたMO媒体であること、ＭＳＮ（＝４５６）が付与されたMO装置であること、ＤＳＮ（＝７８９）が付与されたＭＰＥＧ２デコーダであること、という三つの条件がすべて満たされた場合にのみ、コンテンツ１４１の再生が許諾される。逆に言えば、上記三つの条件のうち一つまたは二つの条件が満たされない場合には、コンテンツ１４１の再生が許諾されない。つまり、ＡＣ１４２は、上記三つの条件を同時に満たすことができる正当な者に対してのみコンテンツ１４１の再生を許諾させるライセンスとしての役目をしている。

【００３９】また、コンテンツ１４１とＡＣ１４２は、図２に示したように関連づけられた状態でMO媒体１４０に格納されている。MO媒体１４０において、コンテンツ１４１は、コンテンツ（１／３）141_1、コンテンツ（２／３）141_2、コンテンツ（３／３）141_3という具合に三分割されている。これらのコンテンツ（１／３）141_1、コンテンツ（２／３）141_2、コンテンツ（３／３）141_3は、ＬＢＮ（Logical Block Number：論理ブロック番号）＝Ｌ、ＬＢＮ＝Ｍおよ

びＬＢＮ＝Ｎでそれぞれ指定された領域に格納されている。

【００４０】同様にして、MO媒体１４０において、ＡＣ１４２は、ＡＣ（１／２）142_1、ＡＣ（２／２）142_2という具合に二分割されている。これらのＡＣ（１／２）142_1、ＡＣ（２／２）142_2は、ＬＢＮ＝Ｘ、ＬＢＮ＝Ｙでそれぞれ指定された領域に格納されている。

【００４１】また、コンテンツ１４１とＡＣ１４２とは、ファイル管理データD_{A1}および補助ファイル管理データD_{A2}を介して関連付けられている。ファイル管理データD_{A1}は、ファイル本体としてのコンテンツ１４１および補助ファイルとしてのＡＣ１４２を管理するためのデータである。このファイル管理データD_{A1}は、「ファイル名」、「作成日時」、…「補助ファイル管理データへのリンク」、「ファイル本体へのリンク（１／３）」、「ファイル本体へのリンク（２／３）」および「ファイル本体へのリンク（３／３）」という情報から構成されている。

【００４２】一方、補助ファイル管理データD_{A2}は、ＡＣ１４２を直接、管理するためのデータであり、「補助ファイル名」、「作成日時」、…、「ＡＣへのリンク（１／２）」、「ＡＣへのリンク（２／２）」という情報から構成されている。

【００４３】図３は、ＡＣ１４２（図１参照）のフォーマットの一例を示す図である。この図において、フラグF_4は、MO媒体ＡＣ：ＭＳＮ＝１２３（図１参照）が論理和（オア）／論理積条件（アンド条件）でないことを示すものである。フラグF_5は、MO装置ＡＣ：ＤＳＮ＝４５６（図１参照）が論理和／論理積条件でないことを示すものである。フラグF_3は、上記MO媒体ＡＣ：ＭＳＮ＝１２３とMO装置ＡＣ：ＤＳＮ＝４５６とが論理和条件であることを示すものである。この場合、論理和条件の個数は２である。

【００４４】フラグF_6は、ＭＰＥＧ２デコーダＡＣ：ＤＳＮ＝７８９が論理和／論理積条件条件でないことを示すものである。フラグF_2は、フラグF_3に関する要素（ＭＳＮ＝１２３、ＤＳＮ＝４５６）と、フラグF_6に関する要素（ＤＳＮ＝７８９）とが論理和条件であることを示すものである。この場合、論理和条件の個数は２である。ここで、図１に示したＡＣ１４２においては、上述したフラグF_2からフラグF_6までのフォーマットが用いられている。したがって、図３に示したフラグF_1、フラグF_7～フラグF_9は、拡張用である。

【００４５】フラグF_8は、MO媒体ＡＣ：ＭＳＮ＝ａｂｃが論理和／論理積条件でないことを示すものである。フラグF_9は、MO装置ＡＣ：ＤＳＮ＝ｄｅｆが論理和／論理積条件でないことを示すものである。フラグF_7は、フラグF_8に関する要素（ＭＳＮ＝ａｂｃ）とフラグF_9に関する要素（ＤＳＮ＝ｄｅｆ）とが論理積条件であることを示すものである。この場合の論理積条件の個数は２である。フラグF_1は、フラグF_2に関する要素（ＭＳＮ＝１２３、ＤＳＮ＝４５６、ＤＳＮ＝７８９）と、フラグF_7に関する要素（ＭＳＮ＝ａｂｃ、ＤＳＮ＝ｄｅｆ）とが論理和条件であることを示すものである。この場合、論理和条件の個数は２である。

【００４６】図１に戻り、MO媒体１４０には、自身の識別情報であるＭＳＮ＝１２３が付与されている。MO装置１２０には、自身の識別情報であるＤＳＮ＝４５６が付与されている。ドライブ１２１は、データ読み出し時にMO媒体１４０を回転駆動する。ＡＣチェック部１２２は、MO媒体１４０から読み出されたＭＳＮ＝１２３が、ＡＣ１４２の条件（この場合、ＭＳＮ＝１２３）を満たすか否かをチェックする。同様にして、ＡＣチェック部１２２は、MO装置１２０に付与されたＤＳＮ＝４５６が、ＡＣ１４２の条件（この場合、ＤＳＮ＝４５６）を満たすか否かをチェックする。

【００４７】ＭＰＥＧ２デコーダ１３０は、ＭＰＥＧ２方式によりコンテンツ１４１（動画データ）をデコードすることにより、コンテンツ１４１を再生する。このＭＰＥＧ２デコーダ１３０には、自身の識別情報であるＤＳＮ＝７８９が付与されている。ＡＣチェック部１３１は、ＡＣ１４２の条件（この場合、ＤＳＮ＝７８９）を満たすか否かをチェックする。

【００４８】MO装置１５０は、MO装置１２０に対して別設（または併設）されており、MO媒体（同図の場合、MO媒体１６０）からデータを読み出す。このMO装置１５０において、ドライブ１５１は、MO媒体１６０を回転駆動する。また、MO装置１５０には、自身の識別情報であるＤＳＮ＝ｄｅｆ（図３参照）が付与されている。このＤＳＮ＝ｄｅｆは、MO装置１２０に付与されたＤＳＮ＝４５６と異なる。MO媒体１６０には、自身の識別情報であるＭＳＮ＝ａｂｃが付与されている。このＭＳＮ＝ａｂｃは、MO媒体１４０に付与されているＭＳＮ＝１２３と異なる。

【００４９】つぎに、上述した実施の形態１の動作について図４に示したフローチャートを参照しつつ説明する。この場合、図１に示したMO装置１２０のドライブ１２１には、MO媒体１４０がセットされているものとする。この状態において、図４に示したステップＳＡ１でユーザＵからＭＰＥＧ２再生部１１４に対してＭＰＥＧ２（コンテンツ）の再生が指示されると、ステップＳＡ２では、ＭＰＥＧ２再生部１１４は、ＡＣＭ１１３に対してＭＰＥＧ２（コンテンツ）の再生を指示する。

【００５０】これにより、ステップＳＡ３では、ＡＣＭ１１３は、MO媒体１４０から、ファイルシステム１１２経由でＡＣ１４２を取得した後、ステップＳＡ４へ進む。ステップＳＡ４では、ＡＣＭ１１３は、取得したＡＣ１４２をMO装置１２０のＡＣチェック部１２２へ転送する。これにより、ステップＳＡ５では、ＡＣチェッ

ク部１２２は、MO媒体１４０からＭＳＮ（＝１２３）を取得した後、ステップＳＡ６へ進む。ステップＳＡ６では、ＡＣチェック部１２２は、ＡＣ１４２の条件とＭＳＮ（＝１２３）とが一致するか否かを判断する。

【００５１】具体的には、ＡＣチェック部１２２は、図１に示したＡＣ１４２の内容（この場合、MO媒体：ＭＳＮ＝１２３）とMO媒体１４０から取得したＭＳＮ（＝１２３）とが一致するか否かを判断する。この場合、両者が一致するため、ＡＣチェック部１２２は、ステップＳＡ６の判断結果を「Ｙｅｓ」として、ステップＳＡ７へ進む。

【００５２】一方、ステップＳＡ６の判断結果が「Ｎｏ」である場合、すなわち、両者が一致しない場合、ＡＣチェック部１２２は、ステップＳＡ１７へ進む。ステップＳＡ１７では、ＡＣチェック部１２２は、ＡＣＭ１１３にチェック結果＝ＮＧを返答する。これにより、ステップＳＡ１８では、ＡＣＭ１１３は、ＭＰＥＧ２再生部１１４にチェック結果＝ＮＧを返答した後、一連の処理を終了する。つまり、この場合には、ＡＣ１４２の条件（ＭＳＮ＝１２３）が満たされていないため、MO媒体１４０に記録されたコンテンツ１４１の再生が許諾されない。

【００５３】この場合、ステップＳＡ７では、ＡＣチェック部１２２は、ＡＣＭ１１３に対してステップＳＡ６におけるチェック結果＝ＯＫとともに、ＡＣ１４２を返却する。これにより、ステップＳＡ８では、ＡＣＭ１１３は、ＡＣチェック部１２２にＡＣ１４２を転送する。そして、上記ＡＣ１４２を受信すると、ステップＳＡ９では、ＡＣチェック部１２２は、MO装置１２０よりＤＳＮ（＝４５６）を取得した後、ステップＳＡ１０へ進む。ステップＳＡ１０では、ＡＣチェック部１２２は、ＡＣ１４２の条件とＤＳＮ（＝４５６）とが一致するか否かを判断する。

【００５４】具体的には、ＡＣチェック部１２２は、図１に示したＡＣ１４２の内容（この場合、MO装置：ＤＳＮ＝４５６）とMO装置１２０から取得したＤＳＮ（＝４５６）とが一致するか否かを判断する。この場合、ＡＣチェック部１２２は、両者が一致するため、ステップＳＡ１０の判断結果を「Ｙｅｓ」として、ステップＳＡ１１へ進む。

【００５５】一方、ステップＳＡ１０の判断結果が「Ｎｏ」である場合、言い換えれば、両者が一致しない場合、ＡＣチェック部１２２は、ステップＳＡ１７へ進む。ステップＳＡ１７では、ＡＣチェック部１２２は、ＡＣＭ１１３にチェック結果＝ＮＧを返答する。これにより、ステップＳＡ１８では、ＡＣＭ１１３は、ＭＰＥＧ２再生部１１４にチェック結果＝ＮＧを返答した後、一連の処理を終了する。つまり、この場合には、ＡＣ１４２の条件（ＭＳＮ＝１２３＆ＤＳＮ＝４５６）が満たされていないため、MO媒体１４０に記録されたコンテンツ１４１の再生が許諾されない。

【００５６】この場合、ステップＳＡ１１では、ＡＣチェック部１２２は、ＡＣＭ１１３に対して、ステップＳＡ１０におけるチェック結果＝ＯＫとともにＡＣ１４２を返却する。これにより、ステップＳＡ１２では、ＡＣＭ１１３は、ＭＰＥＧ２デコーダ１３０のＡＣチェック部１３１へＡＣ１４２を転送する。そして、上記ＡＣ１４２を受信すると、ステップＳＡ１３では、ＡＣチェック部１３１は、ＭＰＥＧ２デコーダ１３０よりＤＳＮ（＝７８９）を取得した後、ステップＳＡ１４へ進む。ステップＳＡ１４では、ＡＣチェック部１３１は、ＡＣ１４２の条件とＤＳＮ（＝７８９）とが一致するか否かを判断する。

【００５７】具体的には、ＡＣチェック部１３１は、図１に示したＡＣ１４２の内容（この場合、ＭＰＥＧ２デコーダ：ＤＳＮ＝７８９）とＭＰＥＧ２デコーダ１３０から取得したＤＳＮ（＝７８９）とが一致するか否かを判断する。この場合、ＡＣチェック部１３１は、両者が一致するため、ステップＳＡ１４の判断結果を「Ｙｅｓ」として、ステップＳＡ１５へ進む。

【００５８】一方、ステップＳＡ１４の判断結果が「Ｎｏ」である場合、言い換えれば、両者が一致しない場合、ＡＣチェック部１３１は、ステップＳＡ１７へ進む。ステップＳＡ１７では、ＡＣチェック部１３１は、ＡＣＭ１１３にチェック結果＝ＮＧを返答する。これにより、ステップＳＡ１８では、ＡＣＭ１１３は、ＭＰＥＧ２再生部１１４にチェック結果＝ＮＧを返答した後、一連の処理を終了する。つまり、この場合には、ＡＣ１４２の条件（ＭＳＮ＝１２３＆ＤＳＮ＝４５６＆ＤＳＮ＝７８９）が満たされていないため、MO媒体１４０に記録されたコンテンツ１４１の再生が許諾されない。

【００５９】この場合、ステップＳＡ１５では、ＡＣチェック部１３１は、ステップＳＡ１４のチェック結果＝ＯＫとともにＡＣ１４２をＡＣＭ１１３に返却する。これにより、ステップＳＡ１６では、ＡＣＭ１１３は、ＭＰＥＧ２再生部１１４に対して、ステップＳＡ６、ステップＳＡ１０およびステップＳＡ１４のすべてのチェック結果＝ＯＫを返答した後、一連の処理を終了する。つまり、この場合には、MO媒体１４０に記録されたＡＣ１４２の条件がすべて満たされているため、MO媒体１４０に記録されたコンテンツ１４１の再生が許諾される。

【００６０】したがって、ＭＰＥＧ２再生部１１４は、ドライブ１２１およびファイルシステム１１２を経由してMO媒体１４０からコンテンツ１４１を読み出した後、これをＭＰＥＧ２デコーダ１３０へ転送する。これにより、ＭＰＥＧ２デコーダ１３０においては、コンテンツ１４１が動画再生される。

【００６１】以上説明したように、実施の形態１によれば、ＡＣ１４２とコンテンツ１４１とを関連付けて一つ

のMO媒体１４０に記録し、ＡＣ１４２および識別情報（ＭＳＮ＝１２３等）に基づいて、コンテンツ１４１の利用の制御を行うようにしたので、MO媒体１４０を入手することで同時にＡＣ１４２とコンテンツ１４１とが得られるため、別々に入手していた従来に比して、コンテンツを容易に利用することができる。

【００６２】（実施の形態２）さて、前述した実施の形態１においては、図１に示したＡＣ１４２に対して特に暗号化の処理を施していない例について説明したが、ＡＣ１４２を暗号化することによりセキュリティを高めるようにしてもよい。以下においては、この場合を実施の形態２として説明する。

【００６３】図５は、本発明にかかる実施の形態２の構成を示すブロック図である。この図において、計算機２１０は、ユーザUにより操作されるものであり、ＯＳ２１１を備えている。この計算機２１０においては、ＯＳ２１１により各種プログラムの実行が制御される。ファイルシステム２１２は、計算機２１０で扱われるファイルを管理し、データのリード／ライトを制御する。ＡＣＭ（アクセス制御マネージャ）２１３は、ファイルシステム２１２、ＭＰＥＧ２再生部２１４、MO装置２２０、ＭＰＥＧ２デコーダ２３０相互間のアクセス制御を管理する。

【００６４】ＭＰＥＧ２再生部２１４は、前述したＭＰＥＧ２再生部１１４（図１参照）と同様の機能を備えている。MO装置２２０は、計算機２１０に外付け（または内蔵）されており、MO媒体（同図の場合、MO媒体２４０）からデータを読み取る。

【００６５】このMO媒体２４０には、コンテンツ２４１と許諾情報２４２とが関連付けられた状態で格納されている。このコンテンツ２４１は、ＭＰＥＧ２方式の動画データである。許諾情報２４２は、コンテンツ２４１の再生の許諾に関する情報である。つまり、許諾情報２４２の条件を満たす場合には、コンテンツ２４１の再生が許諾され、一方、許諾情報２４２の条件を満たさない場合には、コンテンツ２４１の再生が許諾されない。この許諾情報２４２は、複数の情報（ＭＳＮ＝１２３、ＤＳＮ＝４５６およびＤＳＮ＝７８９）が複数の暗号鍵により多重暗号化されてなる。この許諾情報２４２のデータ構造の詳細については図７を参照して後述する。

【００６６】ここで、許諾情報２４２の条件は、複数の対象物理要素にそれぞれ付与された識別情報の組み合わせからなる。この対象物理要素としては、コンテンツ２４１を再生するために必要な装置、媒体であり、MO媒体、MO装置、ＭＰＥＧ２装置である。また、識別情報としては、ＭＳＮ（媒体シリアル番号）、ＤＳＮ（装置シリアル番号）である。具体的には、許諾情報２４２においては、MO媒体のＭＳＮが「１２３」、MO装置のＤＳＮが「４５６」、ＭＰＥＧ２デコーダのＤＳＮが「７８９」に設定されている。また、許諾情報２４２においては、ＭＳＮ（＝１２３）＆ＤＳＮ（＝４５６）＆ＤＳＮ（＝７８９）という論理積（アンド）条件が設定されている。

【００６７】つまり、許諾情報２４２によれば、ＭＳＮ（＝１２３）が付与されたMO媒体であること、ＭＳＮ（＝４５６）が付与されたMO装置であること、ＤＳＮ（＝７８９）が付与されたＭＰＥＧ２デコーダであること、という三つの条件がすべて満たされた場合にのみ、コンテンツ２４１の再生が許諾される。逆に言えば、上記三つの条件のうち一つまたは二つの条件が満たされない場合には、コンテンツ２４１の再生が許諾されない。つまり、許諾情報２４２は、上記三つの条件を同時に満たすことができる正当な者に対してのみコンテンツ２４１の再生を許諾させるライセンスとしての役目をしている。

【００６８】また、コンテンツ２４１と許諾情報２４２は、前述した図２と同様にして、図６に示したように関連づけられた状態でMO媒体２４０に格納されている。MO媒体２４０において、コンテンツ２４１は、コンテンツ（１／３）241_1、コンテンツ（２／３）241_2、コンテンツ（３／３）241_3という具合に三分割されている。これらのコンテンツ（１／３）241_1、コンテンツ（２／３）241_2、コンテンツ（３／３）241_3は、ＬＢＮ＝Ｌ、ＬＢＮ＝MおよびＬＢＮ＝Ｎでそれぞれ指定された領域に格納されている。

【００６９】同様にして、MO媒体２４０において、許諾情報２４２は、許諾情報（１／２）242_1、許諾情報（２／２）242_2という具合に二分割されている。これらの許諾情報（１／２）242_1、許諾情報（２／２）242_2は、ＬＢＮ＝Ｘ、ＬＢＮ＝Ｙでそれぞれ指定された領域に格納されている。

【００７０】また、コンテンツ２４１と許諾情報２４２とは、ファイル管理データD_{B1}および補助ファイル管理データD_{B2}を介して関連付けられている。ファイル管理データD_{B1}は、ファイル本体としてのコンテンツ２４１および補助ファイルとしての許諾情報２４２を管理するためのデータである。このファイル管理データD_{B1}は、「ファイル名」、…、「ファイル本体へのリンク（３／３）」という情報から構成されている。一方、補助ファイル管理データD_{B2}は、許諾情報２４２を直接、管理するためのデータであり、「補助ファイル名」、…、「許諾情報へのリンク（１／２）」、「許諾情報へのリンク（２／２）」という情報から構成されている。

【００７１】図５に戻り、MO媒体２４０には、自身の識別情報であるＭＳＮ＝１２３が付与されている。また、MO媒体２４０には、鍵Ｋｅｙ＝ａｂｃが格納されている。この鍵Ｋｅｙ＝ａｂｃは、許諾情報２４２からＭＳＮ＝１２３を復号するためのものである。MO装置２２０には、自身の識別情報であるＤＳＮ＝４５６が付

与されている。また、MO装置２２０には、鍵Ｋｅｙ＝ｄｅｆが格納されている。この鍵Ｋｅｙ＝ｄｅｆは、許諾情報２４２からＤＳＮ＝４５６を復号するためのものである。

【００７２】ドライブ２２１は、データ読み出し時にMO媒体２４０を回転駆動する。復号部２２３は、MO媒体２４０に格納されている鍵Ｋｅｙ＝ａｂｃを用いて、許諾情報２４２からＭＳＮ＝１２３を復号する。さらに、復号部２２３は、MO装置２２０に格納されている復号鍵Ｋｅｙ＝ｄｅｆを用いて、許諾情報２４２からＤＳＮ＝４５６を復号する。

【００７３】ＡＣチェック部２２２は、MO媒体２４０から読み出されたＭＳＮ＝１２３が、許諾情報２４２の条件（この場合、ＭＳＮ＝１２３）を満たすか否かをチェックする。同様にして、ＡＣチェック部２２２は、MO装置２２０に付与されたＤＳＮ＝４５６が、許諾情報２４２の条件（この場合、ＤＳＮ＝４５６）を満たすか否かをチェックする。

【００７４】ＭＰＥＧ２デコーダ２３０は、ＭＰＥＧ２方式によりコンテンツ２４１（動画データ）をデコードすることにより、コンテンツ２４１を再生する。このＭＰＥＧ２デコーダ２３０には、自身の識別情報であるＤＳＮ＝７８９が付与されている。復号部２３２は、ＭＰＥＧ２デコーダ２３０に格納されている鍵Ｋｅｙ＝ｇｈｉを用いて、許諾情報２４２からＤＳＮ＝７８９を復号する。ＡＣチェック部２３１は、許諾情報２４２の条件（この場合、ＤＳＮ＝７８９）を満たすか否かをチェックする。

【００７５】図７は、実施の形態２におけるライセンス（許諾情報２４２）の一例を示す図である。この図において、ＭＰＥＧ２デコーダＡＣ：ＤＳＮ＝７８９は、前述した対象物理要素としてのＭＰＥＧ２デコーダに対応するものであり、鍵Ｋｅｙ＝ｇｈｉにより暗号化されている。また、ＤＳＮ＝７８９は、ＭＰＥＧ２デコーダ２３０（図５参照）にとっての許諾情報である。

【００７６】MO装置ＡＣ：ＤＳＮ＝４５６は、対象物理要素としてのMO装置に対応するものである。このＤＳＮ＝４５６と暗号化されたＤＳＮ＝７８９とは、鍵Ｋｅｙ＝ｄｅｆにより多重暗号化されている。この多重暗号化されたＤＳＮ＝４５６およびＤＳＮ＝７８９は、MO装置２２０（図５参照）にとっての許諾情報である。また、MO媒体ＡＣ：ＭＳＮ＝１２３は、対象物理要素としてのMO媒体に対応するものである。このＭＳＮ＝１２３と多重暗号化されたＤＳＮ＝４５６およびＤＳＮ＝７８９とは、鍵Ｋｅｙ＝ａｂｃにより多重暗号化されている。この多重暗号化されたＭＳＮ＝１２３、ＤＳＮ＝４５６およびＤＳＮ＝７８９は、MO媒体２４０（図５参照）にとっての許諾情報である。

【００７７】つぎに、上述した実施の形態２の動作について図９に示したフローチャートを参照しつつ説明する。この場合、図５に示したMO装置２２０のドライブ２２１には、MO媒体２４０がセットされているものとする。この状態において、図９に示したステップＳＢ１でユーザＵからＭＰＥＧ２再生部２１４に対してＭＰＥＧ２（コンテンツ）の再生が指示されると、ステップＳＢ２では、ＭＰＥＧ２再生部２１４は、ＡＣＭ２１３に対してＭＰＥＧ２（コンテンツ）の再生を指示する。

【００７８】これにより、ステップＳＢ３では、ＡＣＭ２１３は、MO媒体２４０から、ファイルシステム２１２経由で暗号化された図８（ａ）に示した許諾情報２４２を取得した後、ステップＳＢ４へ進む。ステップＳＢ４では、ＡＣＭ２１３は、取得した許諾情報２４２（図８（ａ）参照）をMO装置２２０の復号部２２３へ転送する。これにより、ステップＳＢ５では、復号部２２３は、MO媒体２４０から鍵Ｋｅｙ（＝ａｂｃ＝Ｋ１（図８（ａ）参照））を取得した後、ステップＳＢ６へ進む。

【００７９】ステップＳＢ６では、復号部２２３は、鍵Ｋｅｙ（＝ａｂｃ＝Ｋ１（図８（ａ）参照））を用いて許諾情報２４２を図８（ｂ）に示したように復号した後、ステップＳＢ７へ進む。ここでは、図８（ｂ）に示したようにＭＳＮ（＝１２３）が復号される。ステップＳＢ７では、復号部２２３は、復号された許諾情報２４２をＡＣチェック部２２２へ転送する。

【００８０】これにより、ステップＳＢ８では、ＡＣチェック部２２２は、MO媒体２４０からＭＳＮ（＝１２３）を取得した後、ステップＳＢ９へ進む。ステップＳＢ９では、ＡＣチェック部２２２は、復号された図８（ｂ）に示した許諾情報２４２の条件（ＭＳＮ＝１２３）と上記ＭＳＮ（＝１２３）とが一致するか否かを判断する。この場合、両者が一致するため、ＡＣチェック部２２２は、ステップＳＢ９の判断結果を「Ｙｅｓ」として、ステップＳＢ１０へ進む。

【００８１】一方、ステップＳＢ９の判断結果が「Ｎｏ」である場合、すなわち、両者が一致しない場合、ＡＣチェック部２２２は、ステップＳＢ２６へ進む。ステップＳＢ２６では、ＡＣチェック部２２２は、ＡＣＭ２１３にチェック結果＝ＮＧを返答する。これにより、ステップＳＢ２７では、ＡＣＭ２１３は、ＭＰＥＧ２再生部２１４にチェック結果＝ＮＧを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報２４２に基づく許諾条件（ＭＳＮ＝１２３）が満たされていないため、MO媒体２４０に記録されたコンテンツ２４１の再生が許諾されない。

【００８２】この場合、ステップＳＢ１０では、ＡＣチェック部２２２は、ＡＣＭ２１３に対してステップＳＢ９におけるチェック結果＝ＯＫとともに、図８（ｃ）に示した許諾情報２４２を返却する。これにより、ステップＳＢ１１では、ＡＣＭ２１３は、MO装置２２０の復号部２２３に許諾情報２４２（図８（ｃ）参照）を転送

する。そして、上記許諾情報２４２を受信すると、ステップＳＢ１２では、復号部２２３は、MO装置２２０より鍵Ｋｅｙ（＝ｄｅｆ＝Ｋ２（図８（ｃ）参照））を取得した後、ステップＳＢ１３へ進む。

【００８３】ステップＳＢ１３では、復号部２２３は、鍵Ｋｅｙ（＝ｄｅｆ＝Ｋ２（図８（ｃ）参照））を用いて許諾情報２４２を図８（ｄ）に示したように復号した後、ステップＳＢ１４へ進む。ここでは、図８（ｄ）に示したようにＤＳＮ（＝４５６）が復号される。ステップＳＢ１４では、復号部２２３は、復号された許諾情報２４２（図８（ｄ）参照）をＡＣチェック部２２２へ転送する。

【００８４】これにより、ステップＳＢ１５では、ＡＣチェック部２２２は、MO装置２２０からＤＳＮ（＝４５６）を取得した後、ステップＳＢ１６へ進む。ステップＳＢ１６では、ＡＣチェック部２２２は、復号された許諾情報２４２の条件（ＤＳＮ＝４５６）と上記ＤＳＮ（＝４５６）とが一致するか否かを判断する。この場合、両者が一致するため、ＡＣチェック部２２２は、ステップＳＢ１６の判断結果を「Ｙｅｓ」として、ステップＳＢ１７へ進む。

【００８５】一方、ステップＳＢ１６の判断結果が「Ｎｏ」である場合、言い換えれば、両者が一致しない場合、ＡＣチェック部２２２は、ステップＳＢ２６へ進む。ステップＳＢ２６では、ＡＣチェック部２２２は、ＡＣＭ２１３にチェック結果＝ＮＧを返答する。これにより、ステップＳＢ２７では、ＡＣＭ２１３は、ＭＰＥＧ２再生部２１４にチェック結果＝ＮＧを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報２４２に基づく許諾条件（ＭＳＮ＝１２３＆ＤＳＮ＝４５６）が満たされていないため、MO媒体２４０に記録されたコンテンツ２４１の再生が許諾されない。

【００８６】この場合、ステップＳＢ１７では、ＡＣチェック部２２２は、ＡＣＭ２１３に対して、ステップＳＢ１６におけるチェック結果＝ＯＫとともに図８（ｅ）に示した許諾情報２４２を返却する。これにより、ステップＳＢ１８では、ＡＣＭ２１３は、ＭＰＥＧ２デコーダ２３０の復号部２３２に許諾情報２４２（図８（ｅ）参照）を転送する。そして、上記許諾情報２４２を受信すると、ステップＳＢ１９では、復号部２３２は、ＭＰＥＧ２デコーダ２３０より鍵Ｋｅｙ（＝ｇｈｉ＝Ｋ３（図８（ｅ）参照））を取得した後、ステップＳＢ２０へ進む。

【００８７】ステップＳＢ２０では、復号部２３２は、鍵Ｋｅｙ（＝ｇｈｉ＝Ｋ３（図８（ｅ）参照））を用いて許諾情報２４２を図８（ｆ）に示したように復号した後、ステップＳＢ２１へ進む。ここでは、図８（ｆ）に示したようにＤＳＮ（＝７８９）が復号される。ステップＳＢ２１では、復号部２３２は、復号された許諾情報２４２（図８（ｆ）参照）をＡＣチェック部２３１へ転送する。

【００８８】これにより、ステップＳＢ２２では、ＡＣチェック部２３１は、ＭＰＥＧ２デコーダ２３０からＤＳＮ（＝７８９）を取得した後、ステップＳＢ２３へ進む。ステップＳＢ２３では、ＡＣチェック部２３１は、復号された許諾情報２４２の条件（ＤＳＮ＝７８９）と上記ＤＳＮ（＝７８９）とが一致するか否かを判断する。この場合、両者が一致するため、ＡＣチェック部２３１は、ステップＳＢ２３の判断結果を「Ｙｅｓ」として、ステップＳＢ２４へ進む。

【００８９】一方、ステップＳＢ２３の判断結果が「Ｎｏ」である場合、言い換えれば、両者が一致しない場合、ＡＣチェック部２３１は、ステップＳＢ２６へ進む。ステップＳＢ２６では、ＡＣチェック部２３１は、ＡＣＭ２１３にチェック結果＝ＮＧを返答する。これにより、ステップＳＢ２７では、ＡＣＭ２１３は、ＭＰＥＧ２再生部２１４にチェック結果＝ＮＧを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報２４２に基づく許諾条件（ＭＳＮ＝１２３＆ＤＳＮ＝４５６＆ＤＳＮ＝７８９）が満たされていないため、MO媒体２４０に記録されたコンテンツ２４１の再生が許諾されない。

【００９０】この場合、ステップＳＢ２４では、ＡＣチェック部２３１は、ステップＳＢ２３のチェック結果＝ＯＫをＡＣＭ２１３に返答する。これにより、ステップＳＢ２５では、ＡＣＭ２１３は、ＭＰＥＧ２再生部２１４に対して、ステップＳＢ９、ステップＳＢ１６およびステップＳＢ２３のすべてのチェック結果＝ＯＫを返答した後、一連の処理を終了する。つまり、この場合には、MO媒体２４０に記録された許諾情報２４２の条件がすべて満たされているため、MO媒体２４０に記録されたコンテンツ２４１の再生が許諾される。

【００９１】したがって、ＭＰＥＧ２再生部２１４は、ドライブ２２１およびファイルシステム２１２を経由してMO媒体２４０からコンテンツ２４１を読み出した後、これをＭＰＥＧ２デコーダ２３０へ転送する。これにより、ＭＰＥＧ２デコーダ２３０においては、コンテンツ２４１が動画再生される。

【００９２】以上説明したように、実施の形態２によれば、図７に示したように複数の部分許諾情報（ＭＳＮ１２３、ＤＳＮ＝４５６等）を多重暗号化してMO媒体２４０に記録するようにしたので、コンテンツ２４１の不正利用を防止することができる。

【００９３】（実施の形態３）さて、前述した実施の形態２においては、図５に示したコンテンツ２４１を暗号化しない例について説明したが、このコンテンツ２４１を暗号化するようにしてもよい。この場合には、暗号化されたコンテンツ２４１を復号するためのコンテンツ復号鍵および許諾情報２４２を多重暗号化してもよい。以下においては、この場合を実施の形態３として説明す

る。

【００９４】図１０は、本発明にかかる実施の形態３の構成を示すブロック図である。この図において、図５の各部に対応する部分には同一の符号を付ける。図１０においては、図５に示したＭＰＥＧ２デコーダ２３０に代えてＭＰＥＧ２デコーダ３１０が設けられている。さらに図１０に示したMO媒体２４０には、図５に示した許諾情報２４２に代えて許諾情報３００が格納されている。ここで、図１０に示したコンテンツ２４１は、暗号化されている。この暗号化されたコンテンツ２４１と許諾情報３００とは、前述した図６の場合と同様にして関連付けられた状態でMO媒体２４０に格納されている。

【００９５】ＭＰＥＧ２デコーダ３１０は、ＡＣチェック部３１１により設定されるコンテンツ復号鍵K_cを用いて、暗号化されたコンテンツ２４１（動画データ）を復号し、この復号された結果をデコードすることにより、コンテンツ２４１を再生する。このＭＰＥＧ２デコーダ３１０には、自身の識別情報であるＤＳＮ＝７８９が付与されている。復号部３１２は、ＭＰＥＧ２デコーダ３１０に格納されている鍵Ｋｅｙ＝ｇｈｉを用いて、許諾情報３００からＭＳＮ＝７８９を復号する。ＡＣチェック部３１１は、許諾情報３００の条件（この場合、ＤＳＮ＝７８９）を満たすか否かをチェックする。

【００９６】図１１は、実施の形態３におけるライセンス（許諾情報３００）の一例を示す図である。この図において、ＭＰＥＧ２デコーダＡＣ：ＤＳＮ＝７８９およびコンテンツ復号鍵K_cは、前述した対象物理要素としてのＭＰＥＧ２デコーダにそれぞれ対応するものであり、鍵Ｋｅｙ＝ｇｈｉにより暗号化されている。このコンテンツ復号鍵K_cは、暗号化されたコンテンツ２４１（図１０参照）をＭＰＥＧ２デコーダ３１０において復号するときに用いられる。また、ＤＳＮ＝７８９およびコンテンツ復号鍵K_cは、ＭＰＥＧ２デコーダ３１０（図１０参照）にとっての許諾情報である。

【００９７】MO装置ＡＣ：ＤＳＮ＝４５６は、対象物理要素としてのMO装置に対応するものである。このＤＳＮ＝４５６と暗号化されたＤＳＮ＝７８９およびコンテンツ復号鍵K_cとは、鍵Ｋｅｙ＝ｄｅｆにより多重暗号化されている。この多重暗号化されたＤＳＮ＝４５６、ＤＳＮ＝７８９およびコンテンツ復号鍵K_cは、ＭＯ装置２２０（図１０参照）にとっての許諾情報である。

【００９８】また、MO媒体ＡＣ：ＭＳＮ＝１２３は、対象物理要素としてのMO媒体に対応するものである。このＭＳＮ＝１２３と、多重暗号化されたＤＳＮ＝４５６、ＤＳＮ＝７８９およびコンテンツ復号鍵K_cとは、鍵Ｋｅｙ＝ａｂｃにより多重暗号化されている。この多重暗号化されたＭＳＮ＝１２３、ＤＳＮ＝４５６、ＤＳＮ＝７８９およびコンテンツ復号鍵K_cは、MO媒体２４０（図１参照）にとっての許諾情報である。

【００９９】つぎに、上述した実施の形態３の動作について図１３に示したフローチャートを参照しつつ説明する。この場合、図１０に示したMO装置２２０のドライブ２２１には、MO媒体２４０がセットされているものとする。この状態において、図１３に示したステップＳＣ１でユーザUからＭＰＥＧ２再生部２１４に対してＭＰＥＧ２（コンテンツ）の再生が指示されると、ステップＳＣ２では、ＭＰＥＧ２再生部２１４は、ＡＣＭ２１３に対してＭＰＥＧ２（コンテンツ）の再生を指示する。

【０１００】これにより、ステップＳＣ３では、ＡＣＭ２１３は、MO媒体２４０から、ファイルシステム２１２経由で暗号化された図１２（ａ）に示した許諾情報３００を取得した後、ステップＳＣ４へ進む。ステップＳＣ４では、ＡＣＭ２１３は、取得した許諾情報３００（図１２（ａ）参照）をMO装置２２０の復号部２２３へ転送する。これにより、ステップＳＣ５では、復号部２２３は、MO媒体２４０から鍵Ｋｅｙ（＝ａｂｃ＝Ｋ１（図１２（ａ）参照））を取得した後、ステップＳＣ６へ進む。

【０１０１】ステップＳＣ６では、復号部２２３は、鍵Ｋｅｙ（＝ａｂｃ＝Ｋ１（図１２（ａ）参照））を用いて許諾情報３００を図１２（ｂ）に示したように復号した後、ステップＳＣ７へ進む。ここでは、図１２（ｂ）に示したようにＭＳＮ（＝１２３）が復号される。ステップＳＣ７では、復号部２２３は、復号された許諾情報３００をＡＣチェック部２２２へ転送する。

【０１０２】これにより、ステップＳＣ８では、ＡＣチェック部２２２は、MO媒体２４０からＭＳＮ（＝１２３）を取得した後、ステップＳＣ９へ進む。ステップＳＣ９では、ＡＣチェック部２２２は、復号された図１２（ｂ）に示した許諾情報３００の条件（ＭＳＮ＝１２３）と上記ＭＳＮ（＝１２３）とが一致するか否かを判断する。この場合、両者が一致するため、ＡＣチェック部２２２は、ステップＳＣ９の判断結果を「Ｙｅｓ」として、ステップＳＣ１０へ進む。

【０１０３】一方、ステップＳＣ９の判断結果が「Ｎｏ」である場合、すなわち、両者が一致しない場合、ＡＣチェック部２２２は、ステップＳＣ２７へ進む。ステップＳＣ２７では、ＡＣチェック部２２２は、ＡＣＭ２１３にチェック結果＝ＮＧを返答する。これにより、ステップＳＣ２８では、ＡＣＭ２１３は、ＭＰＥＧ２再生部２１４にチェック結果＝ＮＧを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報３００に基づく許諾条件（ＭＳＮ＝１２３）が満たされていないため、MO媒体２４０に記録されたコンテンツ２４１の再生が許諾されない。

【０１０４】この場合、ステップＳＣ１０では、ＡＣチェック部２２２は、ＡＣＭ２１３に対してステップＳＣ９におけるチェック結果＝ＯＫとともに、図１２（ｃ）

に示した許諾情報３００を返却する。これにより、ステップＳＣ１１では、ＡＣＭ２１３は、ＭＯ装置２２０の復号部２２３に許諾情報３００（図１２（ｃ）参照）を転送する。そして、上記許諾情報３００を受信すると、ステップＳＣ１２では、復号部２２３は、ＭＯ装置２２０より鍵Ｋｅｙ（＝ｄｅｆ＝Ｋ２（図１２（ｃ）参照））を取得した後、ステップＳＣ１３へ進む。

【０１０５】ステップＳＣ１３では、復号部２２３は、鍵Ｋｅｙ（＝ｄｅｆ＝Ｋ２（図１２（ｃ）参照））を用いて許諾情報３００を図１２（ｄ）に示したように復号した後、ステップＳＣ１４へ進む。ここでは、図１２（ｄ）に示したようにＤＳＮ（＝４５６）が復号される。ステップＳＣ１４では、復号部２２３は、復号された許諾情報３００（図１２（ｄ）参照）をＡＣチェック部２２２へ転送する。

【０１０６】これにより、ステップＳＣ１５では、ＡＣチェック部２２２は、ＭＯ装置２２０からＤＳＮ（＝４５６）を取得した後、ステップＳＣ１６へ進む。ステップＳＣ１６では、ＡＣチェック部２２２は、復号された許諾情報３００の条件（ＤＳＮ＝４５６）と上記ＤＳＮ（＝４５６）とが一致するか否かを判断する。この場合、両者が一致するため、ＡＣチェック部２２２は、ステップＳＣ１６の判断結果を「Ｙｅｓ」として、ステップＳＣ１７へ進む。

【０１０７】一方、ステップＳＣ１６の判断結果が「Ｎｏ」である場合、言い換えれば、両者が一致しない場合、ＡＣチェック部２２２は、ステップＳＣ２７へ進む。ステップＳＣ２７では、ＡＣチェック部２２２は、ＡＣＭ２１３にチェック結果＝ＮＧを返答する。これにより、ステップＳＣ２８では、ＡＣＭ２１３は、ＭＰＥＧ２再生部２１４にチェック結果＝ＮＧを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報３００に基づく許諾条件（ＭＳＮ＝１２３＆ＤＳＮ＝４５６）が満たされていないため、ＭＯ媒体２４０に記録されたコンテンツ２４１の再生が許諾されない。

【０１０８】この場合、ステップＳＣ１７では、ＡＣチェック部２２２は、ＡＣＭ２１３に対して、ステップＳＣ１６におけるチェック結果＝ＯＫとともに図１２（ｅ）に示した許諾情報３００を返却する。これにより、ステップＳＣ１８では、ＡＣＭ２１３は、ＭＰＥＧ２デコーダ３１０の復号部３１２に許諾情報３００（図１２（ｅ）参照）を転送する。そして、上記許諾情報３００を受信すると、ステップＳＣ１９では、復号部３１２は、ＭＰＥＧ２デコーダ３１０より鍵Ｋｅｙ（＝ｇｈｉ＝Ｋ３（図１２（ｅ）参照））を取得した後、ステップＳＣ２０へ進む。

【０１０９】ステップＳＣ２０では、復号部３１２は、鍵Ｋｅｙ（＝ｇｈｉ＝Ｋ３（図１２（ｅ）参照））を用いて許諾情報３００を図１２（ｆ）に示したように復号した後、ステップＳＣ２１へ進む。ここでは、図１２（ｆ）に示したようにＤＳＮ（＝７８９）が復号される。ステップＳＣ２１では、復号部３１２は、復号された許諾情報３００（図１２（ｆ）参照）をＡＣチェック部３１１へ転送する。

【０１１０】これにより、ステップＳＣ２２では、ＡＣチェック部３１１は、ＭＰＥＧ２デコーダ３１０からＤＳＮ（＝７８９）を取得した後、ステップＳＣ２３へ進む。ステップＳＣ２３では、ＡＣチェック部３１１は、復号された許諾情報３００の条件（ＤＳＮ＝７８９）と上記ＤＳＮ（＝７８９）とが一致するか否かを判断する。この場合、両者が一致するため、ＡＣチェック部３１１は、ステップＳＣ２３の判断結果を「Ｙｅｓ」として、ステップＳＣ２４へ進む。

【０１１１】一方、ステップＳＣ２３の判断結果が「Ｎｏ」である場合、言い換えれば、両者が一致しない場合、ＡＣチェック部３１１は、ステップＳＣ２７へ進む。ステップＳＣ２７では、ＡＣチェック部３１１は、ＡＣＭ２１３にチェック結果＝ＮＧを返答する。これにより、ステップＳＣ２８では、ＡＣＭ２１３は、ＭＰＥＧ２再生部２１４にチェック結果＝ＮＧを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報３００に基づく許諾条件（ＭＳＮ＝１２３＆ＤＳＮ＝４５６＆ＤＳＮ＝７８９）が満たされていないため、ＭＯ媒体２４０に記録されたコンテンツ２４１の再生が許諾されない。

【０１１２】この場合、ステップＳＣ２４では、ＡＣチェック部３１１は、ＭＰＥＧ２デコーダ３１０にコンテンツ復号鍵K_cを設定した後、ステップＳＣ２５へ進む。ステップＳＣ２５では、ＡＣチェック部３１１は、ステップＳＣ２３のチェック結果＝ＯＫをＡＣＭ２１３に返答する。これにより、ステップＳＣ２６では、ＡＣＭ２１３は、ＭＰＥＧ２再生部２１４に対して、ステップＳＣ９、ステップＳＣ１６およびステップＳＣ２３のすべてのチェック結果＝ＯＫを返答した後、一連の処理を終了する。つまり、この場合には、ＭＯ媒体２４０に記録された許諾情報３００の条件がすべて満たされているため、ＭＯ媒体２４０に記録されたコンテンツ２４１の再生が許諾される。

【０１１３】したがって、ＭＰＥＧ２再生部２１４は、ドライブ２２１およびファイルシステム２１２を経由してＭＯ媒体２４０から暗号化されたコンテンツ２４１を読み出した後、これをＭＰＥＧ２デコーダ３１０へ転送する。これにより、ＭＰＥＧ２デコーダ３１０においては、ステップＳＣ２４で設定されたコンテンツ復号鍵K_cを用いて復号されたコンテンツ２４１が動画再生される。

【０１１４】以上説明したように、実施の形態３によれば、図１１に示したように複数の部分許諾情報（ＭＳＮ＝１２３、ＤＳＮ＝４５６等）に加えてコンテンツ２４１を復号するためのコンテンツ復号鍵K_cを多重暗号

化してMO媒体２４０に記録するようにしたので、コンテンツ２４１の不正利用をより効果的に防止することができる。

【０１１５】（実施の形態４）前述した実施の形態３においては、図１０に示したファイルシステム２１２がMO媒体２４０から許諾情報を無条件で読み出す例について説明したが、セキュリティをさらに高める目的で、MO媒体２４０上のセキュア領域（暗号化領域）に暗号化された許諾情報を格納し、この暗号化された許諾情報を復号することができるファイルシステムのみが許諾情報を読み出すことができるようにしてもよい。以下においては、この場合を実施の形態４として説明する。

【０１１６】図１４は、本発明にかかる実施の形態４の構成を示すブロック図である。この図において、図１０の各部に対応する部分には同一の符号を付ける。図１４においては、図１０に示したMO媒体２４０および計算機２１０に代えて、MO媒体４４０および計算機４００が設けられている。

【０１１７】図１４に示したMO媒体４４０は、図１５に示したように、暗号化されたコンテンツ４４１が格納される非セキュア領域A_1と、暗号化された許諾情報４４２が格納されるセキュア領域A_2とを有している。ここで、非セキュア領域A_1は、ユーザ領域であり、一般のファイルシステムであればアクセス可能な領域である。一方、セキュア領域A_2は、一般のファイルシステムがアクセスできない領域であり、図１４に示した復号器４１１を有するファイルシステム４１０のみがアクセス可能な領域である。

【０１１８】図１５に示した許諾情報４４２は、前述した許諾情報３００（図１０および図１１参照）が暗号化されたものである。したがって、許諾情報４４２には、図１１に示したMSN＝１２３、DSN＝４５６、DSN＝７８９およびコンテンツ復号鍵K_cが含まれている。また、図１５において、許諾情報４４２は、補助ファイル管理データD_{C2}により管理される。

【０１１９】一方、非セキュア領域A_1において、ファイル管理データD_{C1}は、コンテンツ４４１を管理するためのデータであるとともに、補助ファイル管理データD_{C2}を介して許諾情報４４２を間接的に管理するためのデータである。このように、MO媒体４４０においては、コンテンツ４４１と許諾情報４４２がファイル管理データD_{C1}および補助ファイル管理データD_{C2}を介して関連付けられている。図１４に戻り、計算機４００のファイルシステム４１０は、MO媒体４４０から許諾情報４４２、コンテンツ４４１、鍵Ｋｅｙ＝ａｂｃ、MSN＝１２３をそれぞれ読み出す。復号器４１１は、暗号化された許諾情報４４２を復号する。

【０１２０】つぎに、上述した実施の形態４の動作について図１６および図１７に示したフローチャートを参照しつつ説明する。この場合、図１４に示したMO装置２２０のドライブ２２１には、MO媒体４４０がセットされているものとする。この状態において、図１６に示したステップＳＤ１でユーザUからＭＰＥＧ２再生部２１４に対してＭＰＥＧ２（コンテンツ）の再生が指示されると、ステップＳＤ２では、ＭＰＥＧ２再生部２１４は、ＡＣＭ２１３に対してＭＰＥＧ２（コンテンツ）の再生を指示する。

【０１２１】これにより、ステップＳＤ３では、ファイルシステム４１０は、MO媒体４４０のセキュア領域A_2（図１５参照）にアクセスし、暗号化された許諾情報４４２を取得した後、これを復号器４１１へ渡す。ステップＳＤ４では、復号器４１１は、暗号化された許諾情報４４２（図１５参照）を所定の鍵を用いて復号した後、ステップＳＤ５へ進む。ステップＳＤ５では、復号器４１１は、復号された許諾情報４４２をＡＣＭ２１３に転送する。

【０１２２】これにより、図１７に示したステップＳＤ６では、ＡＣＭ２１３は、復号された許諾情報４４２をMO装置２２０の復号部２２３に転送する。ステップＳＤ７では、復号部２２３は、MO媒体４４０から鍵Ｋｅｙ（＝ａｂｃ＝Ｋ１（図１２（ａ）参照））を取得した後、ステップＳＤ８へ進む。ステップＳＤ８では、復号部２２３は、鍵Ｋｅｙ（＝ａｂｃ）を用いて許諾情報４４２を図１２（ｂ）に示したように復号した後、ステップＳＤ９へ進む。ここでは、図１２（ｂ）に示したようにＭＳＮ（＝１２３）が復号される。ステップＳＤ９では、復号部２２３は、復号された許諾情報４４２をＡＣチェック部２２２へ転送する。

【０１２３】これにより、ステップＳＤ１０では、ＡＣチェック部２２２は、MO媒体４４０からＭＳＮ（＝１２３）を取得した後、ステップＳＤ１１へ進む。ステップＳＤ１１では、ＡＣチェック部２２２は、復号された図１２（ｂ）に示した許諾情報４４２の条件（ＭＳＮ＝１２３）と上記ＭＳＮ（＝１２３）とが一致するか否かを判断する。この場合、両者が一致するため、ＡＣチェック部２２２は、ステップＳＤ１１の判断結果を「Ｙｅｓ」として、ステップＳＤ１２へ進む。

【０１２４】一方、ステップＳＤ１１の判断結果が「Ｎｏ」である場合、すなわち、両者が一致しない場合、ＡＣチェック部２２２は、ステップＳＤ２９へ進む。ステップＳＤ２９では、ＡＣチェック部２２２は、ＡＣＭ２１３にチェック結果＝ＮＧを返答する。これにより、ステップＳＤ３０では、ＡＣＭ２１３は、ＭＰＥＧ２再生部２１４にチェック結果＝ＮＧを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報４４２に基づく許諾条件（ＭＳＮ＝１２３）が満たされていないため、MO媒体４４０に記録されたコンテンツ４４１の再生が許諾されない。

【０１２５】この場合、ステップＳＤ１２では、ＡＣチェック部２２２は、ＡＣＭ２１３に対してステップＳＤ

１１におけるチェック結果＝ＯＫとともに、許諾情報４４２（図１２（ｃ）参照）を返却する。これにより、ステップＳＤ１３では、ＡＣＭ２１３は、ＭＯ装置２２０の復号部２２３に許諾情報４４２（図１２（ｃ）参照）を転送する。そして、上記許諾情報４４２を受信すると、ステップＳＤ１４では、復号部２２３は、ＭＯ装置２２０より鍵Ｋｅｙ（＝ｄｅｆ＝Ｋ２（図１２（ｃ）参照））を取得した後、ステップＳＤ１５へ進む。

【０１２６】ステップＳＤ１５では、復号部２２３は、鍵Ｋｅｙ（＝ｄｅｆ＝Ｋ２（図１２（ｃ）参照））を用いて許諾情報４４２を図１２（ｄ）に示したように復号した後、ステップＳＤ１６へ進む。ここでは、図１２（ｄ）に示したようにＤＳＮ（＝４５６）が復号される。ステップＳＤ１６では、復号部２２３は、復号された許諾情報４４２（図１２（ｄ）参照）をＡＣチェック部２２２へ転送する。

【０１２７】これにより、ステップＳＤ１７では、ＡＣチェック部２２２は、ＭＯ装置２２０からＤＳＮ（＝４５６）を取得した後、ステップＳＤ１８へ進む。ステップＳＤ１８では、ＡＣチェック部２２２は、復号された許諾情報４４２の条件（ＤＳＮ＝４５６）と上記ＤＳＮ（＝４５６）とが一致するか否かを判断する。この場合、両者が一致するため、ＡＣチェック部２２２は、ステップＳＤ１８の判断結果を「Ｙｅｓ」として、ステップＳＤ１９へ進む。

【０１２８】一方、ステップＳＤ１８の判断結果が「Ｎｏ」である場合、言い換えれば、両者が一致しない場合、ＡＣチェック部２２２は、ステップＳＤ２９へ進む。ステップＳＤ２９では、ＡＣチェック部２２２は、ＡＣＭ２１３にチェック結果＝ＮＧを返答する。これにより、ステップＳＤ３０では、ＡＣＭ２１３は、ＭＰＥＧ２再生部２１４にチェック結果＝ＮＧを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報４４２に基づく許諾条件（ＭＳＮ＝１２３＆ＤＳＮ＝４５６）が満たされていないため、ＭＯ媒体４４０に記録されたコンテンツ４４１の再生が許諾されない。

【０１２９】この場合、ステップＳＤ１９では、ＡＣチェック部２２２は、ＡＣＭ２１３に対して、ステップＳＤ１８におけるチェック結果＝ＯＫとともに図１２（ｅ）に示した許諾情報４４２を返却する。これにより、ステップＳＤ２０では、ＡＣＭ２１３は、ＭＰＥＧ２デコーダ３１０の復号部３１２に許諾情報４４２（図１２（ｅ）参照）を転送する。そして、上記許諾情報４４２を受信すると、ステップＳＤ２１では、復号部３１２は、ＭＰＥＧ２デコーダ３１０より鍵Ｋｅｙ（＝ｇｈｉ＝Ｋ３（図１２（ｅ）参照））を取得した後、ステップＳＤ２２へ進む。

【０１３０】ステップＳＤ２２では、復号部３１２は、鍵Ｋｅｙ（＝ｇｈｉ＝Ｋ３（図１２（ｅ）参照））を用いて許諾情報４４２を図１２（ｆ）に示したように復号した後、ステップＳＤ２３へ進む。ここでは、図１２（ｆ）に示したようにＤＳＮ（＝７８９）が復号される。ステップＳＤ２３では、復号部３１２は、復号された許諾情報４４２（図１２（ｆ）参照）をＡＣチェック部３１１へ転送する。

【０１３１】これにより、ステップＳＤ２４では、ＡＣチェック部３１１は、ＭＰＥＧ２デコーダ３１０からＤＳＮ（＝７８９）を取得した後、ステップＳＤ２５へ進む。ステップＳＤ２５では、ＡＣチェック部３１１は、復号された許諾情報４４２の条件（ＤＳＮ＝７８９）と上記ＤＳＮ（＝７８９）とが一致するか否かを判断する。この場合、両者が一致するため、ＡＣチェック部３１１は、ステップＳＤ２５の判断結果を「Ｙｅｓ」として、ステップＳＤ２６へ進む。

【０１３２】一方、ステップＳＤ２５の判断結果が「Ｎｏ」である場合、言い換えれば、両者が一致しない場合、ＡＣチェック部３１１は、ステップＳＤ２９へ進む。ステップＳＤ２９では、ＡＣチェック部３１１は、ＡＣＭ２１３にチェック結果＝ＮＧを返答する。これにより、ステップＳＤ３０では、ＡＣＭ２１３は、ＭＰＥＧ２再生部２１４にチェック結果＝ＮＧを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報４４２に基づく許諾条件（ＭＳＮ＝１２３＆ＤＳＮ＝４５６＆ＤＳＮ＝７８９）が満たされていないため、ＭＯ媒体４４０に記録されたコンテンツ４４１の再生が許諾されない。

【０１３３】この場合、ステップＳＤ２６では、ＡＣチェック部３１１は、ＭＰＥＧ２デコーダ３１０にコンテンツ復号鍵K_cを設定した後、ステップＳＤ２７へ進む。ステップＳＤ２７では、ＡＣチェック部３１１は、ステップＳＤ２６のチェック結果＝ＯＫをＡＣＭ２１３に返答する。これにより、ステップＳＤ２８では、ＡＣＭ２１３は、ＭＰＥＧ２再生部２１４に対して、ステップＳＤ１１、ステップＳＤ１８およびステップＳＤ２５のすべてのチェック結果＝ＯＫを返答した後、一連の処理を終了する。つまり、この場合には、ＭＯ媒体４４０に記録された許諾情報４４２の条件がすべて満たされているため、ＭＯ媒体４４０に記録されたコンテンツ４４１の再生が許諾される。

【０１３４】したがって、ＭＰＥＧ２再生部２１４は、ドライブ２２１およびファイルシステム４１０を経由してＭＯ媒体４４０から暗号化されたコンテンツ４４１を読み出した後、これをＭＰＥＧ２デコーダ３１０へ転送する。これにより、ＭＰＥＧ２デコーダ３１０においては、ステップＳＤ２６で設定されたコンテンツ復号鍵K_cを用いて復号されたコンテンツ４４１が動画再生される。

【０１３５】つぎに、図１４に示した許諾情報４４２を、コンテンツ４４１、鍵Ｋｅｙ＝ａｂｃおよびＭＳＮ＝１２３が既に格納されているＭＯ媒体４４０に書き込

むデータ書込装置について、図１８を参照しつつ説明する。つまり、MO媒体４４０には、許諾情報４４２が格納されていない。この図において、計算機４６０は、駅、コンビニエンスストア等に設置されており、許諾情報を購入する装置である。この計算機４６０においては、許諾情報を購入するための許諾情報購入アプリケーションプログラム４６１が起動される。ＯＳ４６２は、許諾情報購入アプリケーションプログラム４６１を制御する。

【０１３６】ファイルシステム４６３は、計算機４６０で扱われるファイルを管理し、データのリード／ライトを制御する。暗号器４６４は、MO媒体４４０に対して書き込むべきデータを暗号化する。ライセンスサーバ４５０は、コンテンツ提供者側に設置されており、ネットワークNを介して計算機４６０に接続されている。このライセンスサーバ４５０は、許諾情報を販売するためのものである。MO装置４７０は、計算機４６０に外付け（または内蔵）されており、MO媒体（同図の場合、MO媒体４４０）に対してデータを書き込む。このMO装置４７０は、MO媒体を駆動するドライブ４７１を有している。

【０１３７】つぎに、図１９を参照して図１８に示したデータ書込装置の動作について説明する。この図に示したステップＳＥ１では、ユーザUは、図示しない入力装置を用いて、ファイル名（たとえば、曲名）、サーバ名等のパラメータを入力することにより、許諾情報４４２の購入を指示する。これにより、ステップＳＥ２では、許諾情報購入アプリケーションプログラム４６１は、ネットワークNを介してライセンスサーバ４５０から許諾情報４４２を購入（取得）した後、ステップＳＥ３へ進む。

【０１３８】ステップＳＥ３では、許諾情報購入アプリケーションプログラム４６１は、許諾情報４４２をファイルシステム４６３へ転送する。これにより、ステップＳＥ４では、ファイルシステム４６３の暗号器４６４は、所定の鍵を用いて許諾情報４４２を暗号化する。つぎのステップＳＥ５では、ファイルシステム４６３は、MO装置４７０を経由してMO媒体４４０のセキュア領域A_2（図１５参照）に暗号化された許諾情報４４２を格納する。

【０１３９】以上説明したように、実施の形態４によれば、図１５に示したように、MO媒体４４０のセキュア領域A_2に暗号化された許諾情報４４２を記録するようにしたので、コンテンツ４４１の不正利用を防止することができる。

【０１４０】（実施の形態５）図２０は、本発明にかかる実施の形態５の構成を示すブロック図である。この図において、図１０の各部に対応する部分には同一の符号を付ける。図２０においては、図１０に示したMO媒体２４０、計算機２１０およびMO装置２２０に代えて、MO媒体５４０、計算機５００およびMO装置５２０が設けられている。

【０１４１】図２０に示したMO媒体５４０は、図２１に示したように、通常領域B_1、特別領域B_2および媒体管理用領域B_3を有している。通常領域B_1は、コンテンツ５４１（図２０参照）が格納される領域であり、この通常領域B_1の範囲は、ＰＳＮ（Physical Sector Number：物理セクタ番号）＝Ｍ＋１～Ｎまでとされている。特別領域B_2は、後述する相互認証コマンド（特別なコマンド）が発行された場合にのみアクセスが可能な領域であり、許諾情報５４２（図２０参照）が格納されている。この許諾情報５４２は、前述した許諾情報３００と同一のデータ構造（図１１参照）である。また、この特別領域B_2の範囲は、ＰＳＮ＝Ｌ～Ｍまでとされている。

【０１４２】媒体管理用領域B_3には、MO媒体５４０における通常領域B_1および特別領域B_2の範囲を定義する媒体管理テーブルＴが格納されている。この媒体管理テーブルＴには、通常領域B_1および特別領域B_2の開始ＰＳＮ（物理セクタ番号における先頭番号）と、通常領域B_1および特別領域B_2の終了ＰＳＮ（物理セクタ番号における末尾番号）とがそれぞれ定義されている。また、この媒体管理用領域B_3の範囲は、ＰＳＮ＝１～Ｌまでとされている。

【０１４３】図２０に戻り、MO媒体５４０には、上述したコンテンツ５４１、許諾情報５４２の他に、MO媒体２４０（図１０参照）と同様にして、鍵Ｋｅｙ＝ａｂｃ、ＭＳＮ＝１２３がそれぞれ格納されている。計算機５００において、ファイルシステム５１０は、計算機５００で扱われるファイルを管理し、データのリード／ライトを制御する。相互認証モジュール５１１は、MO装置５２０の相互認証モジュール５２１が有する秘密情報（以下、MO装置側秘密情報と称する）と共通の秘密情報（以下、計算機側秘密情報と称する）を保持している。

【０１４４】また、相互認証モジュール５１１は、上述した相互認証コマンドが発行されたとき、相互認証モジュール５２１との間で相互認証を行う。具体的には、相互認証モジュール５１１は、計算機側秘密情報を相互認証モジュール５２１へ送信し、相互認証モジュール５２１からのMO装置側秘密情報と自身が保持する計算機側秘密情報とが一致するか否かにより相互認証を行う。ここで、ファイルシステム５１０は、相互認証された場合にのみMO媒体５４０の特別領域B_2から許諾情報５４２を読み出すことが可能である。

【０１４５】MO装置５２０において、相互認証モジュール５２１は、上述したように、ファイルシステム５１０の相互認証モジュール５１１が有する計算機側秘密情報と共通のMO装置側秘密情報を保持している。相互認証モジュール５２１は、相互認証モジュール５１１から

の計算機側秘密情報を受信したとき、自身が保持するMO装置側秘密情報を相互認証モジュール５１１へ送信する。また、相互認証モジュール５２１は、相互認証モジュール５１１からの計算機側秘密情報と自身が保持するMO装置側秘密情報とが一致するか否かにより相互認証を行う。

【０１４６】つぎに、実施の形態５の動作について、図２２および図１３に示したフローチャートを参照しつつ説明する。この場合、図２０に示したMO装置５２０のドライブ２２１には、MO媒体５４０がセットされているものとする。この状態において、図２２に示したステップＳＦ１でユーザUからＭＰＥＧ２再生部２１４に対してＭＰＥＧ２（コンテンツ）の再生が指示されると、ステップＳＦ２では、ＭＰＥＧ２再生部２１４は、ＡＣＭ２１３に対してＭＰＥＧ２（コンテンツ）の再生を指示する。

【０１４７】これにより、ステップＳＦ３では、ＡＣＭ２１３からファイルシステム５１０に対して相互認証コマンドが発行され、相互認証モジュール５１１と相互認証モジュール５２１との間で相互認証が行われる。すなわち、ファイルシステム５１０の相互認証モジュール５１１は、MO装置５２０の相互認証モジュール５２１へ計算機側秘密情報を送信する。そして、この計算機側秘密情報を受信すると、相互認証モジュール５２１は、相互認証モジュール５１１へMO装置側秘密情報を送信する。

【０１４８】つぎに、相互認証モジュール５２１は、受信した計算機側秘密情報と自身が保有するMO装置側秘密情報とが一致するか否かを判断し、この判断結果を相互認証モジュール５１１へ渡す。一方、相互認証モジュール５１１は、相互認証モジュール５２１からのMO装置側秘密情報を受信すると、受信したMO装置側秘密情報と自身が保持する計算機側秘密情報とが一致するか否かを判断する。

【０１４９】そして、ステップＳＦ４では、ファイルシステム５１０は、相互認証モジュール５１１側の相互認証に関する判断結果と、相互認証モジュール５２１側の相互認証に関する判断結果との双方に基づいて、相互認証がとられたか否かを判断する。ここで、双方の判断結果が共に「一致」である場合、ファイルシステム５１０は、相互認証結果＝ＯＫをＡＣＭ２１３へ渡し、ステップＳＦ４の判断結果を「Ｙｅｓ」とする。

【０１５０】これにより、図１３に示したステップＳＣ３では、ＡＣＭ２１３は、ファイルシステム５１０経由でMO媒体５４０の特別領域B_2から許諾情報５４２を取得する。以後、前述した実施の形態３と同様にして、ステップＳＣ４～ステップＳＣ２８までの処理が実行される。なお、実施の形態５においては、図１３に示したMO媒体２４０、許諾情報３００、コンテンツ２４１、ファイルシステム２１２およびMO装置２２０を、MO媒体５４０、許諾情報５４２、コンテンツ５４１、ファイルシステム５１０およびMO装置５２０と読み替えるものとする。

【０１５１】一方、図２２に示したステップＳＦ４において、相互認証モジュール５１１側の相互認証に関する判断結果と、相互認証モジュール５２１側の相互認証に関する判断結果との双方が共に「不一致」である場合、判断結果を「Ｎｏ」として、図１３に示したステップＳＣ２７へ進む。ステップＳＣ１７では、ファイルシステム５１０は、相互認証結果＝ＮＧをＡＣＭ２１３へ渡す。この場合には、相互認証がとられなかったため、図２０に示したMO媒体５４０の特別領域B_2からは、許諾情報５４２が読み出されることがない。

【０１５２】つぎに、図２０に示したMO媒体５４０に通常領域B_1および特別領域B_2を設定するフォーマット装置について、図２３を参照して説明する。この図に示した計算機５６０は、MO媒体５４０に対して物理フォーマットを行う装置である。フォーマッタ５６１は、MO媒体５４０の物理フォーマットに関する制御を行う。ＯＳ５６２は、各種アプリケーションプログラムを制御する。デバイスドライバ５６３は、MO装置５７０を駆動するものである。MO装置５７０は、計算機５６０に外付け（または内蔵）されている。このMO装置５７０は、MO媒体を駆動するドライブ５７１および物理フォーマットを行う。

【０１５３】つぎに、図２４を参照して図２３に示したフォーマット装置の動作について説明する。この図に示したステップＳＧ１では、ユーザUは、図示しない入力装置を用いて、セキュア領域（特別領域B_2（図２１参照））のサイズを指定することにより、MO媒体５４０のフォーマットを指示する。これにより、ステップＳＧ２では、フォーマッタ５６１は、デバイスドライバ５６３経由で物理フォーマット部５７２に対して物理フォーマットを指示する。これにより、ステップＳＧ３では、物理フォーマット部５７２は、MO媒体５４０に対する物理フォーマットを実行する。これにより、MO媒体５４０には、通常領域B_1および特別領域B_2が形成される。

【０１５４】以上説明したように、実施の形態５によれば、図２１に示したMO媒体５４０の特別領域B_2に許諾情報５４２を記録し、二つの相互認証モジュール５１１、相互認証モジュール５２１で相互認証がとられた場合にのみ、該特別領域B_2から許諾情報５４２を取得するようにしたので、相互認証がとられない場合に、即時に許諾不可とすることができ、コンテンツ５４１の不正利用を防止することができる。

【０１５５】（実施の形態６）さて、前述した実施の形態４においては、図１５に示したようにMO媒体４４０に非セキュア領域A_1およびセキュア領域A_2を確保した例について説明した。また、実施の形態５において

は、図２１に示したようにMO媒体５４０に通常領域B_1および特別領域B_2を確保した例について説明した。以下においては、実施の形態４（非セキュア領域A_1、セキュア領域A_2）と実施の形態５（通常領域B_1、特別領域B_2）とを組み合わせた例を実施の形態６として説明する。

【０１５６】実施の形態６においては、図２５に示したMO媒体６００が用いられる。すなわち、同図に示したMO媒体６００においては、通常領域B_1（図２１参照）と非セキュア領域A_1（図１５参照）とがマッピングされているとともに、特別領域B_2（図２１参照）とセキュア領域A_2（図１５参照）とがマッピングされている。また、通常領域B_1（非セキュア領域A_1）には、コンテンツ４４１およびこれを管理するためのファイル管理データD_{C1}が格納されている。一方、特別領域B_2（セキュア領域A_2）には、許諾情報４４２およびこれを管理するための補助ファイル管理データD_{C2}が格納されている。

【０１５７】以上説明したように、実施の形態６によれば、いずれもセキュリティ上有効である特別領域B_2にセキュア領域A_2をマッピングするようにしたので、極めて高いセキュリティを確保することができる。

【０１５８】（実施の形態７）さて、前述した実施の形態１～６においては、MO媒体に格納されたコンテンツおよび許諾情報（ＡＣ）を別のMO媒体に転送するようにしてもよい。以下、この場合を実施の形態７として説明する。図２６は、本発明にかかる実施の形態７におけるパックドデータ生成装置の構成を示すブロック図であり、図２７は、同実施の形態７におけるアンパック装置の構成を示すブロック図である。

【０１５９】これらのパックドデータ生成装置（図２６参照）とアンパック装置（図２７参照）とは図示しないケーブル、ネットワーク等を介して接続されている。図２６に示したパックドデータ生成装置は、MO媒体８００に格納された許諾情報８０１および暗号化コンテンツ８０２をひとまとまりのデータ（パックドデータ８３０）として、これをアンパック装置（図２７参照）へ転送する装置である。

【０１６０】図２６において、MO媒体８００に格納された許諾情報８０１は、前述した実施の形態１～６のうちいずれかの許諾情報（ＡＣ）である。この許諾情報８０１には、ＭＳＮおよび鍵Ｋｅｙが含まれている。暗号化コンテンツ８０２は、暗号化されたコンテンツである。計算機８２０は、送信側に設置されている。ＯＳ８２１は、各種アプリケーションプログラムの実行を制御する。ファイルシステム８２２は、計算機８２０で扱われるファイルを管理し、データのリード／ライトを制御する。

【０１６１】パック処理部８２３は、許諾情報８０１と暗号化コンテンツ８０２とから一つのファイル（パックドデータ８３０）を生成する。転送部８２４は、パックドデータ８３０をアンパック装置（図２７参照）転送する。MO装置８１０は、計算機８２０に外付け（または内蔵）されており、MO媒体（同図の場合、MO媒体８００）から許諾情報８０１および暗号化コンテンツ８０２を読み出す。このMO装置８１０は、MO媒体を駆動するドライブ８１１を有している。

【０１６２】一方、図２７において、計算機９２０は、受信側に設置されている。ＯＳ９２１は、各種アプリケーションプログラムの実行を制御する。ファイルシステム９２２は、計算機９２０で扱われるファイルを管理し、データのリード／ライトを制御する。受信部９２４は、パックドデータ生成装置（図２６参照）から転送されたパックドデータ８３０を受信する。アンパック処理部９２３は、上記パックドデータ８３０から二つのファイル（許諾情報８０１、暗号化コンテンツ８０２）を生成する。MO装置９１０は、計算機９２０に外付け（または内蔵）されており、MO媒体（同図の場合、MO媒体９００）に許諾情報８０１および暗号化コンテンツ８０２を書き込む。このMO装置９１０は、MO媒体を駆動するドライブ９１１を有している。

【０１６３】上記構成において、図２６に示したMO媒体８００から許諾情報８０１および暗号化コンテンツ８０２が読み出されると、パック処理部８２３は、これら許諾情報８０１と暗号化コンテンツ８０２とから一つのファイル（パックドデータ８３０）を生成し、これを転送部８２４へ渡す。これにより、転送部８２４は、ケーブル、ネットワーク等を介して図２７に示したアンパック装置へパックドデータ８３０転送する。

【０１６４】そして、パックドデータ８３０が図２７に示した受信部９２４に受信されると、アンパック処理部９２３は、パックドデータ８３０から許諾情報８０１および暗号化コンテンツ８０２を生成する。これにより、MO媒体９００には、許諾情報８０１および暗号化コンテンツ８０２が書き込まれる。このようにして、実施の形態７においては、MO媒体８００からMO媒体９００へ許諾情報８０１および暗号化コンテンツ８０２を転送（コピー）できるようにしたので、コンテンツの再生に関する許諾（ライセンス）を容易に譲渡することができる。

【０１６５】以上説明したように、実施の形態７によれば、一方のメディア８００から他方のメディア９００へ暗号化コンテンツ８０２および許諾情報８０１が転送（コピー）されるので、コンテンツ８０１の利用に関する許諾（ライセンス）を第三者に譲渡することができる。

【０１６６】以上本発明にかかる実施の形態１～７について図面を参照して詳述してきたが、具体的な構成例はこれら実施の形態１～７に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等があっても本発

明に含まれる。

【０１６７】たとえば、前述した実施の形態１～７においては、コンテンツ利用制御装置、利用制御システムの機能を実現するためのコンテンツ利用制御プログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたコンテンツ利用制御プログラムをコンピュータに読み込ませ、実行することによりコンテンツ利用制御を行うようにしてもよい。なお、記録媒体には、光ディスク、フロッピーディスク、ハードディスク等の可搬型の記録媒体が含まれることはもとより、ネットワークのようにデータを一時的に記録保持するような伝送媒体も含まれる。

【０１６８】

【発明の効果】以上説明したように、請求項１、８にかかる発明によれば、許諾情報とコンテンツとを関連付けて一つのメディアに記録し、この許諾情報および識別情報に基づいて、コンテンツの利用の制御を行うようにしたので、一つのメディアを入手することで同時に許諾情報とコンテンツとが得られるため、許諾情報とコンテンツと別々に入手していた従来に比して、コンテンツを容易に利用することができるという効果を奏する。

【０１６９】また、請求項２にかかる発明によれば、複数の部分許諾情報を多重暗号化してメディアに記録するようにしたので、コンテンツの不正利用を防止することができるという効果を奏する。

【０１７０】また、請求項３にかかる発明によれば、複数の部分許諾情報に加えてコンテンツを復号するためのコンテンツ復号鍵を多重暗号化してメディアに記録するようにしたので、コンテンツの不正利用をより効果的に防止することができるという効果を奏する。

【０１７１】また、請求項４にかかる発明によれば、メディアのセキュア領域に暗号化された許諾情報を記録するようにしたので、コンテンツの不正利用を防止することができるという効果を奏する。

【０１７２】また、請求項５にかかる発明によれば、メディアの特別領域に許諾情報を記録し、二つの物理要素間で相互認証がとられた場合にのみ、該特別領域から許諾情報を取得するようにしたので、相互認証がとられない場合に、即時に許諾不可とすることができ、コンテンツの不正利用を防止することができるという効果を奏する。

【０１７３】また、請求項６にかかる発明によれば、いずれもセキュリティ上有効である特別領域にセキュア領域をマッピングするようにしたので、極めて高いセキュリティを確保することができるという効果を奏する。

【０１７４】また、請求項７にかかる発明によれば、一方のメディアから他方のメディアへコンテンツおよび許諾情報が転送（コピー）されるので、コンテンツの利用に関する許諾（ライセンス）を第三者に譲渡することができるという効果を奏する。

【図面の簡単な説明】

【図１】本発明にかかる実施の形態１の構成を示すブロック図である。

【図２】図１に示したコンテンツ１４１とＡＣ１４２との関係を示す図である。

【図３】図１に示したＡＣ１４２のフォーマットの一例を示す図である。

【図４】同実施の形態１の動作を説明するフローチャートである。

【図５】本発明にかかる実施の形態２の構成を示すブロック図である。

【図６】図５に示したコンテンツ２４１と許諾情報２４２との関係を示す図である。

【図７】図５に示したＡＣ２４２のフォーマットの一例を示す図である。

【図８】図５に示した許諾情報２４２の一例を示す図である。

【図９】同実施の形態２の動作を説明するフローチャートである。

【図１０】本発明にかかる実施の形態３の構成を示すブロック図である。

【図１１】同実施の形態３におけるライセンスの一例を示す図である。

【図１２】図１０に示した許諾情報３００の一例を示す図である。

【図１３】同実施の形態３の動作を説明するフローチャートである。

【図１４】本発明にかかる実施の形態４の構成を示すブロック図である。

【図１５】図１４に示したMO媒体４４０におけるデータ構造を示す図である。

【図１６】同実施の形態４の動作を説明するフローチャートである。

【図１７】同実施の形態４の動作を説明するフローチャートである。

【図１８】同実施の形態４におけるデータ書込装置の構成を示すブロック図である。

【図１９】図１８に示したデータ書込装置の動作を説明するフローチャートである。

【図２０】本発明にかかる実施の形態５の構成を示すブロック図である。

【図２１】図２０に示したMO媒体５４０におけるデータ構造を示す図である。

【図２２】同実施の形態５の動作を説明するフローチャートである。

【図２３】同実施の形態５におけるフォーマット装置の構成を示すブロック図である。

【図２４】図２３に示したフォーマット装置の動作を説明するフローチャートである。

【図２５】本発明にかかる実施の形態６におけるMO媒

体６００のデータ構造を説明する図である。

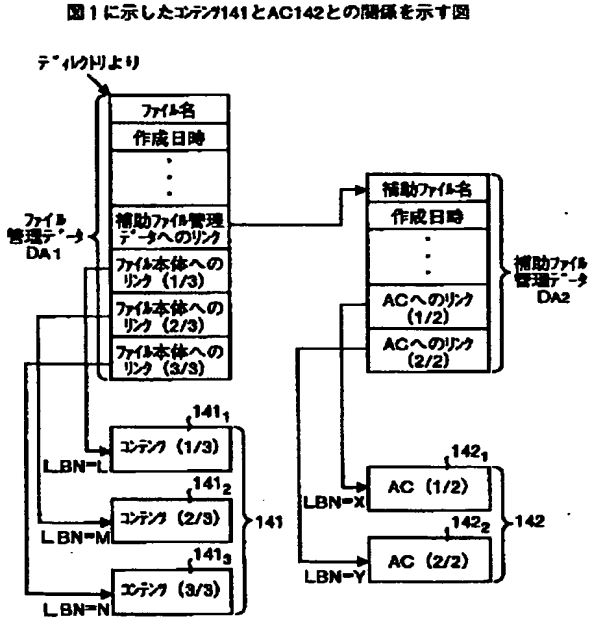
【図２６】本発明にかかる実施の形態７におけるパックドデータ生成装置の構成を示すブロック図である。

【図２７】同実施の形態７におけるアンパック装置の構成を示すブロック図である。

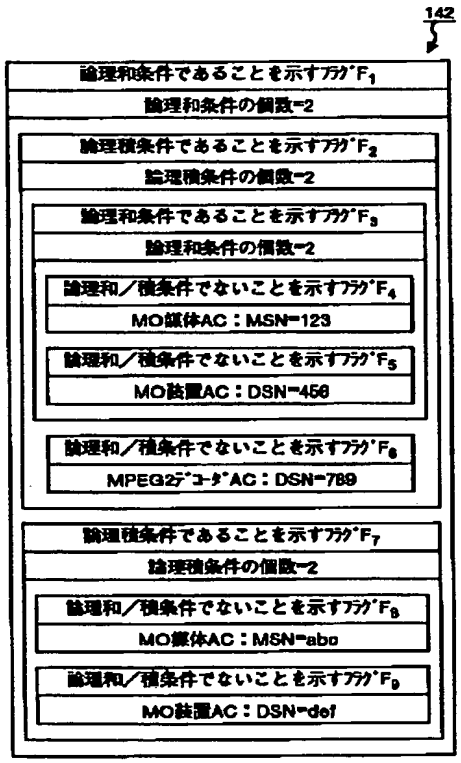
【符号の説明】

１１０　計算機
１１２　ファイルシステム
１１４　ＭＰＥＧ２再生部
１２０　ＭＯ装置
１３０　ＭＰＥＧ２デコーダ
１４０　ＭＯ媒体
２１０　計算機
２２０　ＭＯ装置
２４０　ＭＯ媒体
４００　計算機
４４０　ＭＯ媒体
４００　計算機
５００　計算機
５１１　相互認証モジュール
５２０　ＭＯ装置
５２１　相互認証モジュール
５４０　ＭＯ媒体
５６０　計算機
５７０　ＭＯ装置
８００　ＭＯ媒体
８２０　計算機
８２４　転送部
９２０　計算機
９２４　受信部

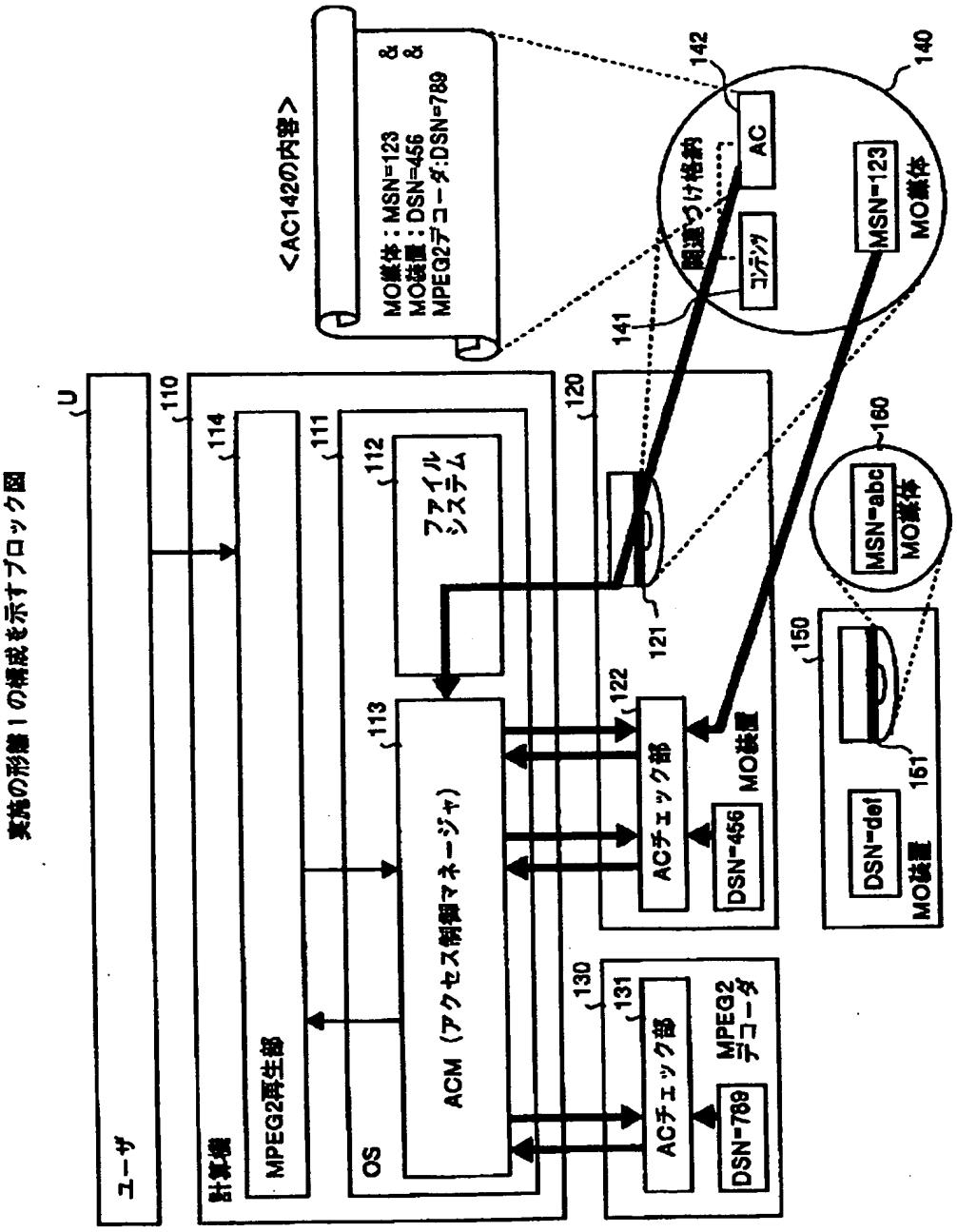
【図２】



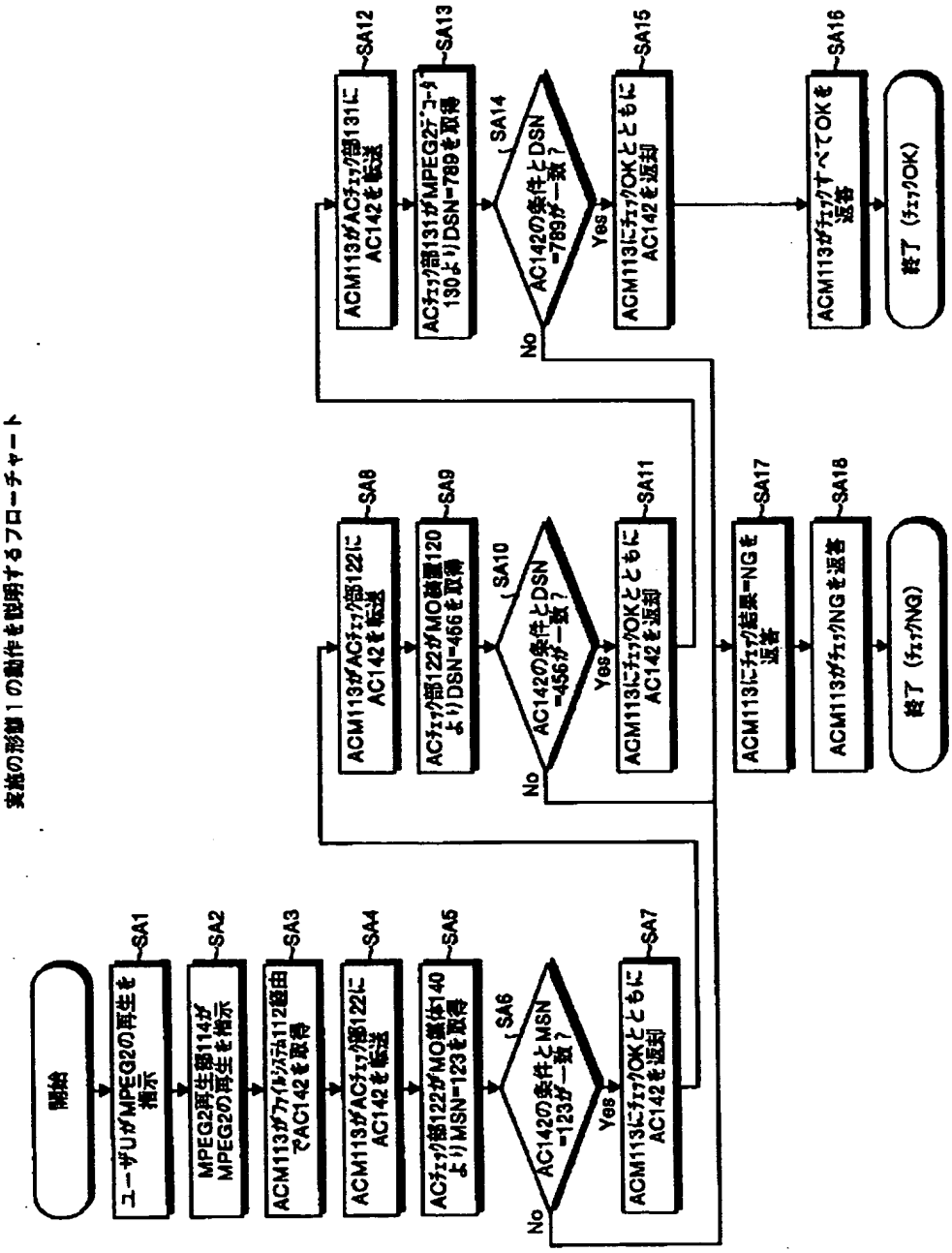
【図３】



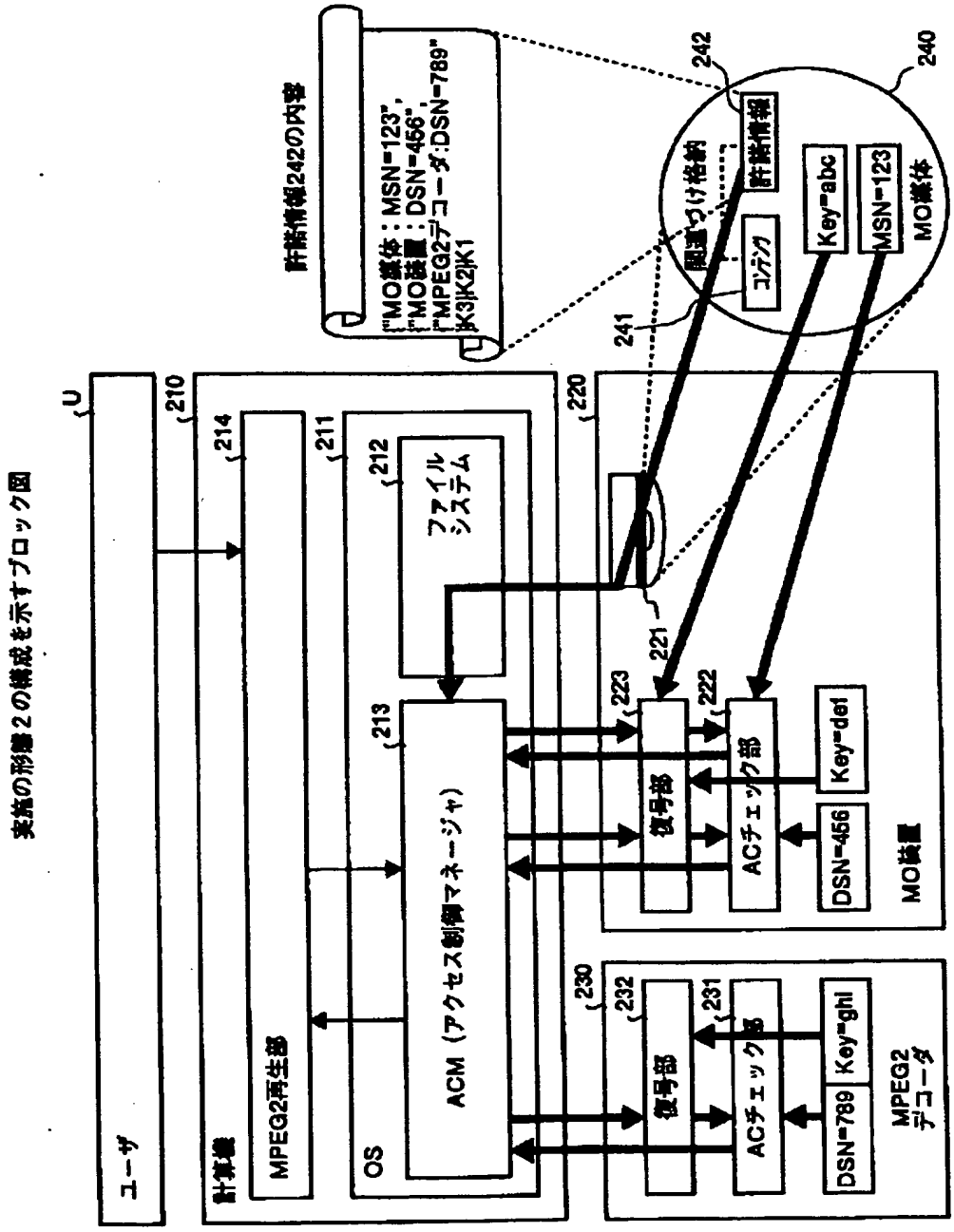
【図１】


実施の形態１の構成を示すブロック図
ユーザ
U
計算機
MPEG2再生部
110
114
OS
ファイルシステム
111
112
ACM（アクセス制御マネージャ）
113
<AC1420の内容>
MO媒体：MSN=123
MO装置：DSN=456
MPEG2デコーダ:DSN=789
&
&
120
121
ACチェック部
122
DSN=456
MO装置
130
131
ACチェック部
MPEG2デコーダ
DSN=789
140
142
関連づけ情報
AC
コンテンツ
141
MSN=123
MO媒体
160
MSN=abc
MO媒体
150
DSN=del
MO装置
151

【図４】

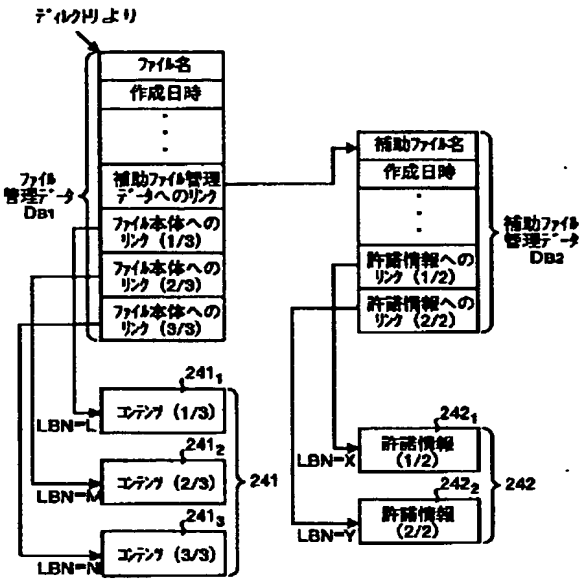

実施の形態１の動作を説明するフローチャート
開始
SA1
ユーザUがMPEG2の再生を指示
SA2
MPEG2再生部114がMPEG2の再生を指示
SA3
ACM113がファイルシステム112経由でAC142を取得
SA4
ACM113がACチェック部122にAC142を転送
SA5
ACチェック部122がMO装置140よりMSN-123を取得
SA6
AC142の条件とMSN=123が一致？
Yes
No
SA7
ACM113にチェックOKとともにAC142を返却
SA8
ACM113がACチェック部122にAC142を転送
SA9
ACチェック部122がMO装置120よりDSN=466を取得
SA10
AC142の条件とDSN=456が一致？
Yes
No
SA11
ACM113にチェックOKとともにAC142を返却
SA12
ACM113がACチェック部131にAC142を転送
SA13
ACチェック部131がMPEG2デコーダ130よりDSN=789を取得
SA14
AC142の条件とDSN=789が一致？
Yes
No
SA15
ACM113にチェックOKとともにAC142を返却
SA16
ACM113がチェックすべてOKを返答
終了（チェックOK）
SA17
ACM113にチェック結果=NGを返答
SA18
ACM113がチェックNGを返答
終了（チェックNG）

【図５】


実施の形態２の構成を示すブロック図
U
ユーザ
210
計算機
214
MPEG2再生部
211
OS
212
ファイルシステム
213
ACM（アクセス制御マネージャ）
220
MO装置
221
223
復号部
222
ACチェック部
Key=del
DSN=456
230
MPEG2デコーダ
232
復号部
231
ACチェック部
DSN=789
Key=ghi
241
242
許諾情報
関連づけ格納
コンテンツ
240
MO媒体
Key=abc
MSN=123
許諾情報2420の内容
{"MO媒体：MSN=123",
"MO装置：DSN=456",
"MPEG2デコーダ:DSN=789"
}K3|K2|K1

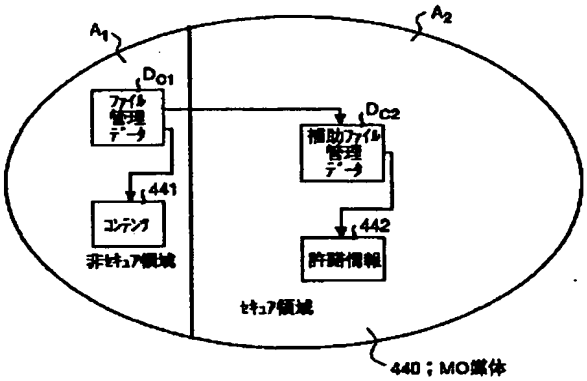
【図６】

図５に示したｺﾝﾃﾝﾂ241と許諾情報242との関係を示す図



【図１５】

図14に示したMO媒体440におけるﾃﾞｰﾀ構造を示す図



【図８】

図５に示した許諾情報242の一例を示す図

(a) ｛“MO媒体：MSN=123”，｛“MO装置：DSN=456”，｛“MPEG2ﾃﾞｺｰﾀﾞ：DSN=789”｝K3｝K2｝K1

(b) “MO媒体：MSN=123”，｛“MO装置：DSN=456”，｛“MPEG2ﾃﾞｺｰﾀﾞ：DSN=789”｝K3｝K2

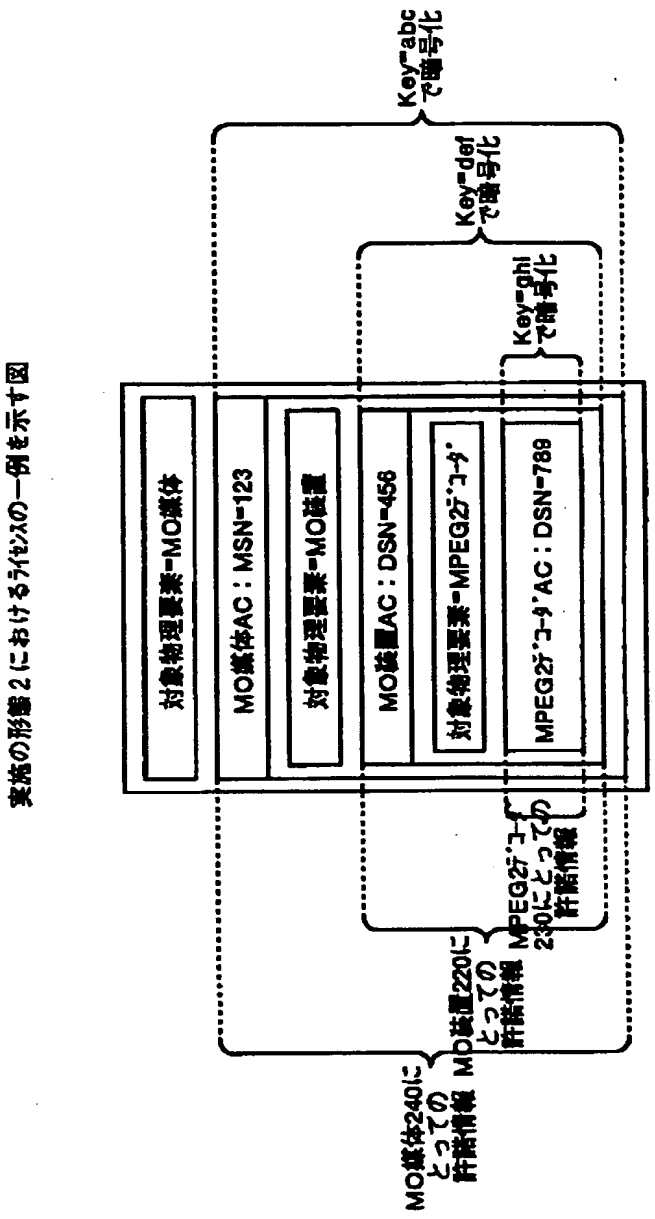
(c) ｛“MO装置：DSN=456”，｛“MPEG2ﾃﾞｺｰﾀﾞ：DSN=789”｝K3｝K2

(d) “MO装置：DSN=456”，｛“MPEG2ﾃﾞｺｰﾀﾞ：DSN=789”｝K3

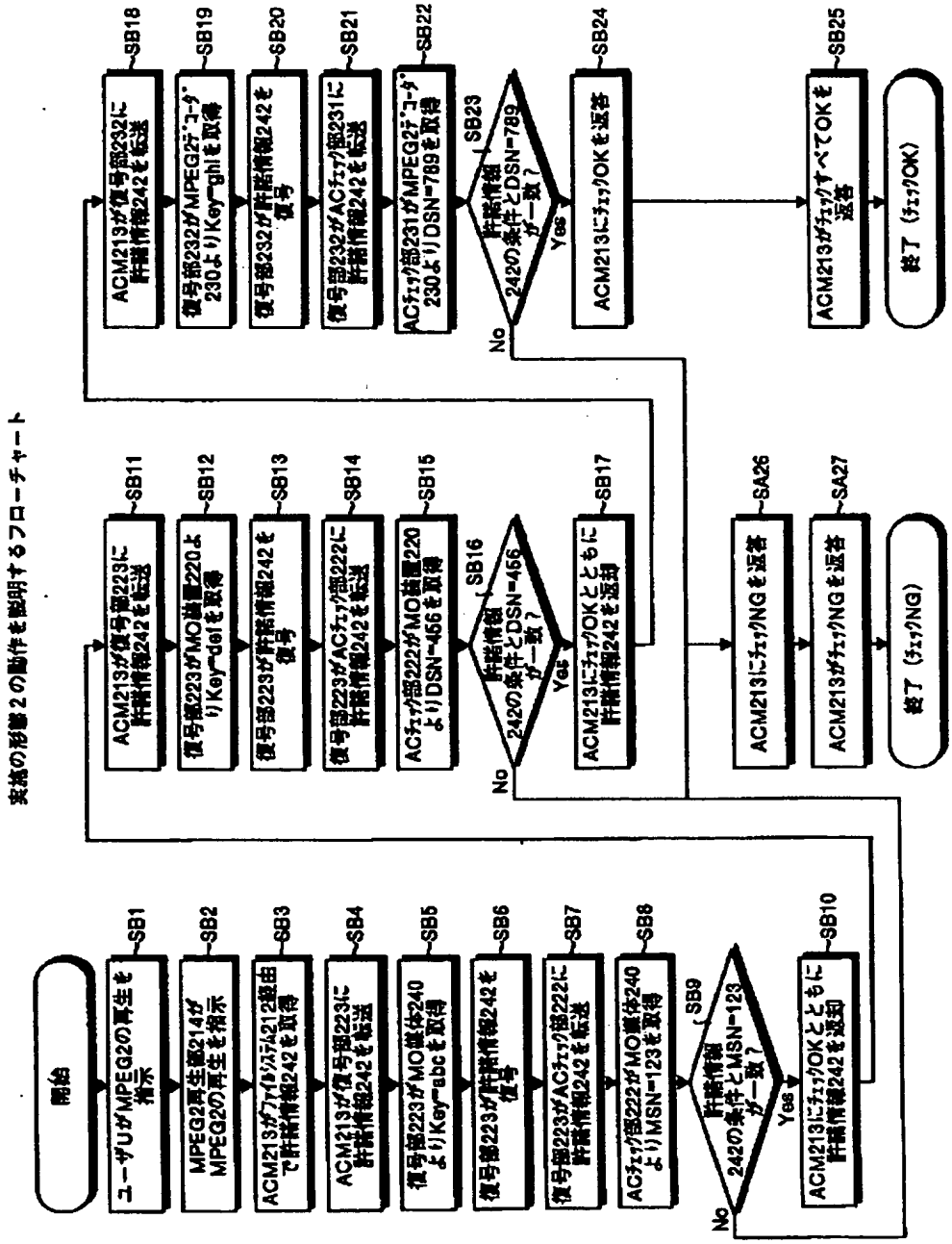
(e) ｛“MPEG2ﾃﾞｺｰﾀﾞ：DSN=789”｝K3

(f) “MPEG2ﾃﾞｺｰﾀﾞ：DSN=789”

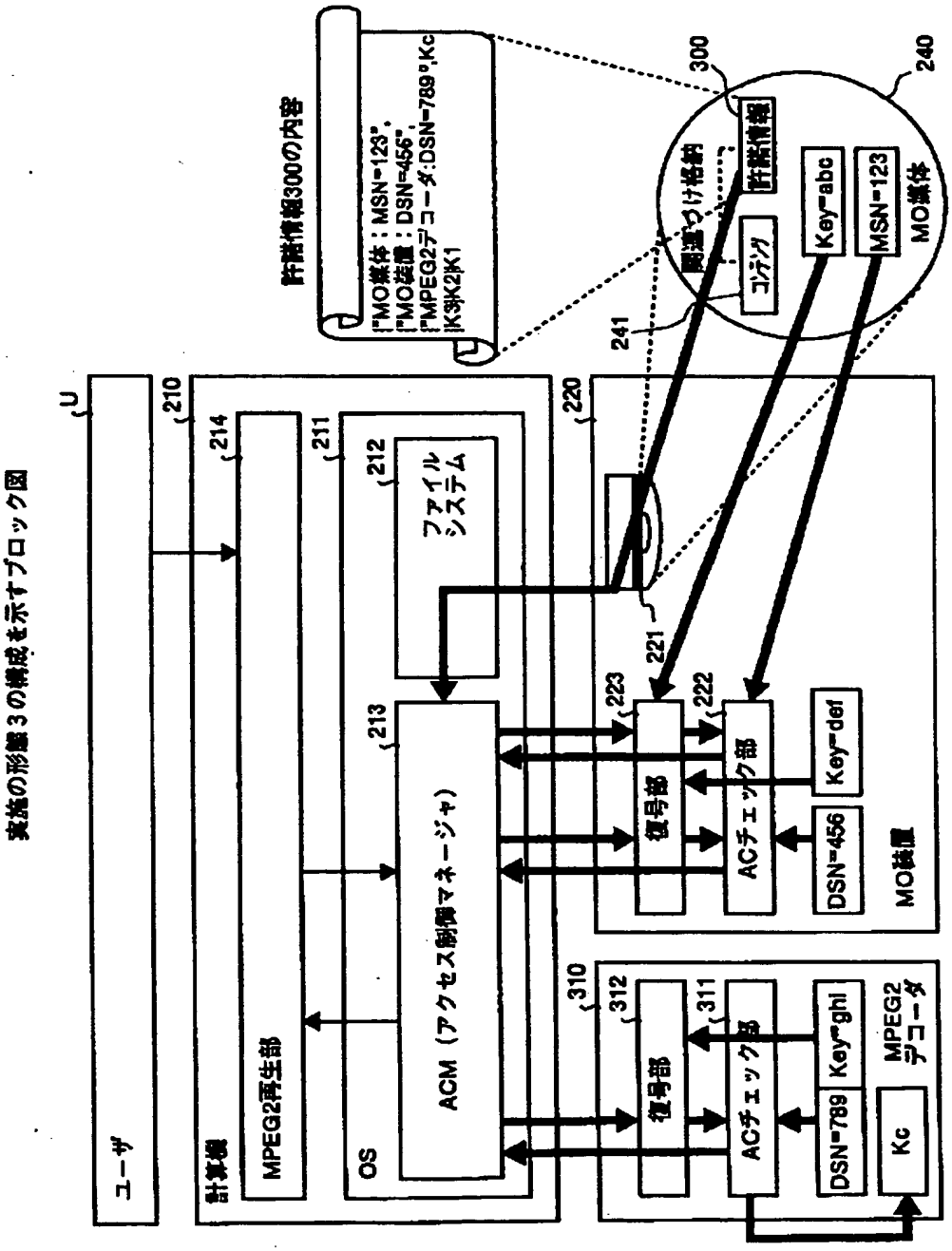
【図７】


実施の形態２におけるライセンスの一例を示す図
対象物理要素=MO媒体
MO媒体AC：MSN=123
対象物理要素=MO装置
MO装置AC：DSN=456
対象物理要素=MPEG2ﾃﾞｺｰﾀﾞ
MPEG2ﾃﾞｺｰﾀﾞAC：DSN=789
Key=abcで暗号化
Key=defで暗号化
Key=ghiで暗号化
MO媒体240にとっての許諾情報
MO装置220にとっての許諾情報
MPEG2ﾃﾞｺｰﾀﾞ230にとっての許諾情報

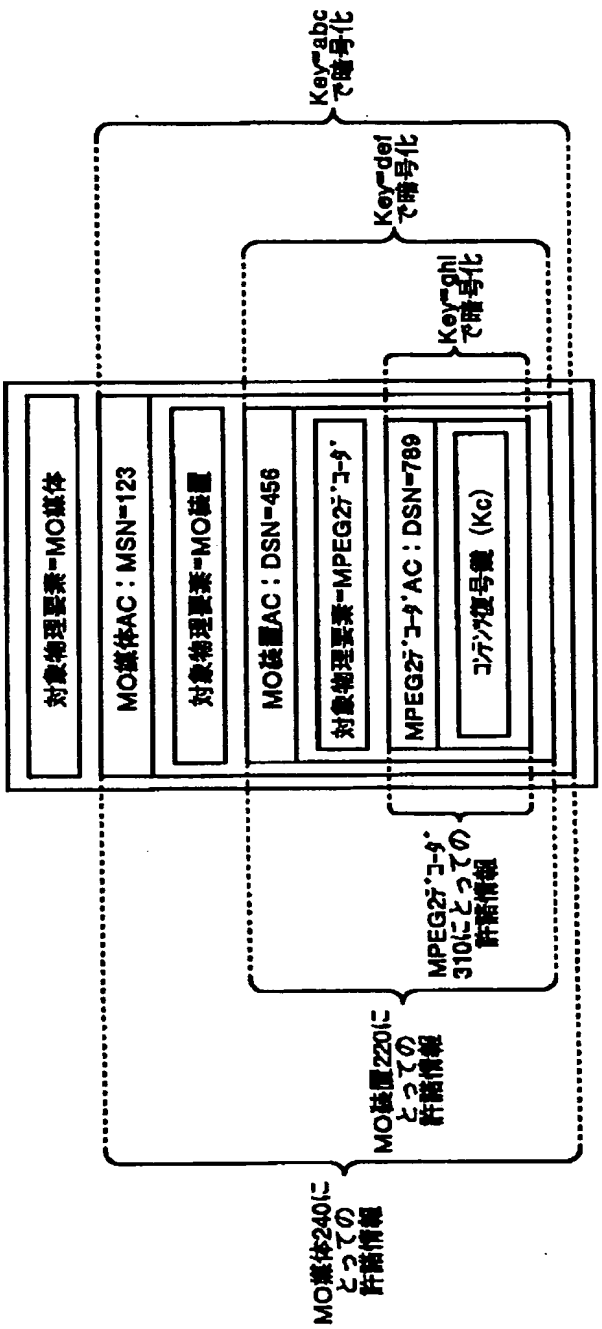
【図９】


実施の形態２の動作を説明するフローチャート
開始
SB1
ユーザUがMPEG2の再生を指示
SB2
MPEG2再生部214がMPEG2の再生を指示
SB3
ACM213がファイルシステム212経由で許諾情報242を取得
SB4
ACM213が復号部223に許諾情報242を転送
SB5
復号部223がMO装置240よりKey-abcを取得
SB6
復号部223が許諾情報242を復号
SB7
復号部223がACチェック部222に許諾情報242を転送
SB8
ACチェック部222がMO装置240よりMSN-123を取得
SB9
許諾情報242の条件とMSN-123が一致？
Yes
No
SB10
ACM213にチェックOKとともに許諾情報242を返却
SB11
ACM213が復号部223に許諾情報242を転送
SB12
復号部223がMO装置220よりKey-defを取得
SB13
復号部223が許諾情報242を復号
SB14
復号部223がACチェック部222に許諾情報242を転送
SB15
ACチェック部222がMO装置220よりDSN-456を取得
SB16
許諾情報242の条件とDSN-456が一致？
Yes
No
SB17
ACM213にチェックOKとともに許諾情報242を返却
SB18
ACM213が復号部232に許諾情報242を転送
SB19
復号部232がMPEG2デコーダ230よりKey-ghiを取得
SB20
復号部232が許諾情報242を復号
SB21
復号部232がACチェック部231に許諾情報242を転送
SB22
ACチェック部231がMPEG2デコーダ230よりDSN-789を取得
SB23
許諾情報242の条件とDSN-789が一致？
Yes
No
SB24
ACM213にチェックOKを返答
SB25
ACM213がチェックすべてOKを返答
終了（チェックOK）
SA26
ACM213にチェックNGを返答
SA27
ACM213がチェックNGを返答
終了（チェックNG）

【図１０】


実施の形態３の構成を示すブロック図
U
ユーザ
210
計算機
214
MPEG2再生部
211
OS
212
ファイルシステム
213
ACM（アクセス制御マネージャ）
220
MO装置
221
223
復号部
222
ACチェック部
Key=def
DSN=456
310
312
復号部
311
ACチェック部
Key=ghi
DSN=789
Kc
MPEG2デコーダ
241
300
許諾情報
コンテンツ
Key=abc
MSN=123
MO媒体
240
許諾情報300の内容
{"MO媒体：MSN=123",
{"MO装置：DSN=456",
{"MPEG2デコーダ:DSN=789",Kc
{K3|K2|K1

【図１１】



実施の形態３におけるライセンスの一例を示す図

【図１２】

図10に示した許諾情報300の一例を示す図

(a) {"MO媒体：MSN=123"，{"MO装置：DSN=456"，{"MPEG2ﾃﾞｺｰﾀﾞ：DSN=789",Kc} K3} K2} K1

(b) "MO媒体：MSN=123"，{"MO装置：DSN=456"，{"MPEG2ﾃﾞｺｰﾀﾞ：DSN=789",Kc} K3} K2

(c) {"MO装置：DSN=456"，{"MPEG2ﾃﾞｺｰﾀﾞ：DSN=789",Kc} K3} K2

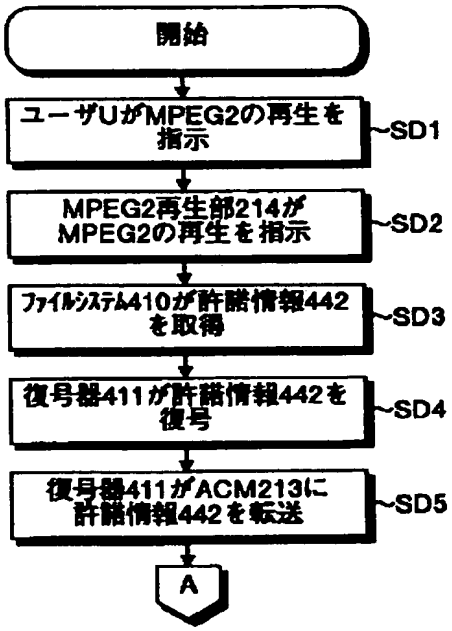
(d) "MO装置：DSN=456"，{"MPEG2ﾃﾞｺｰﾀﾞ：DSN=789",Kc} K3

(e) {"MPEG2ﾃﾞｺｰﾀﾞ：DSN=789",Kc} K3

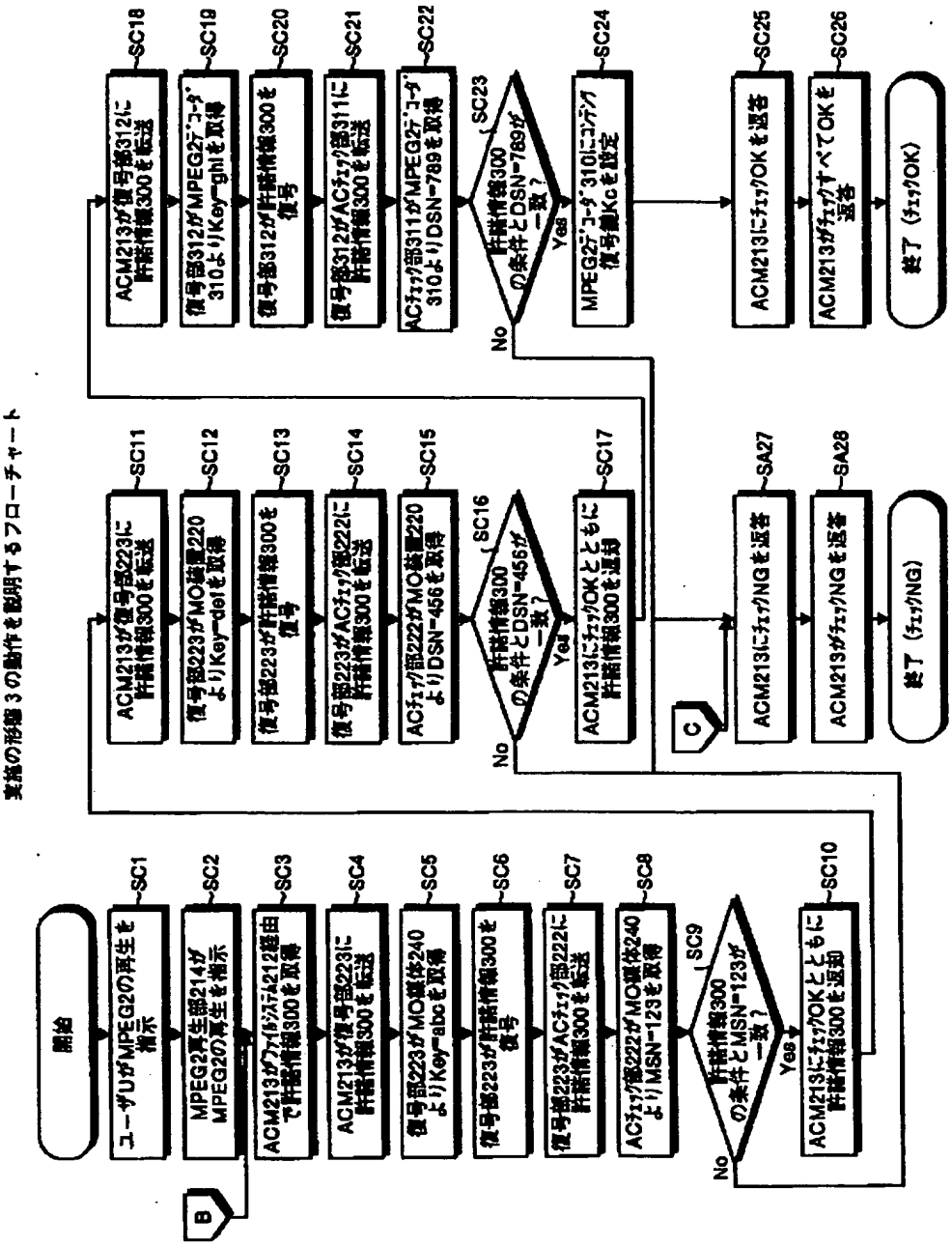
(f) "MPEG2ﾃﾞｺｰﾀﾞ：DSN=789",Kc

【図１６】

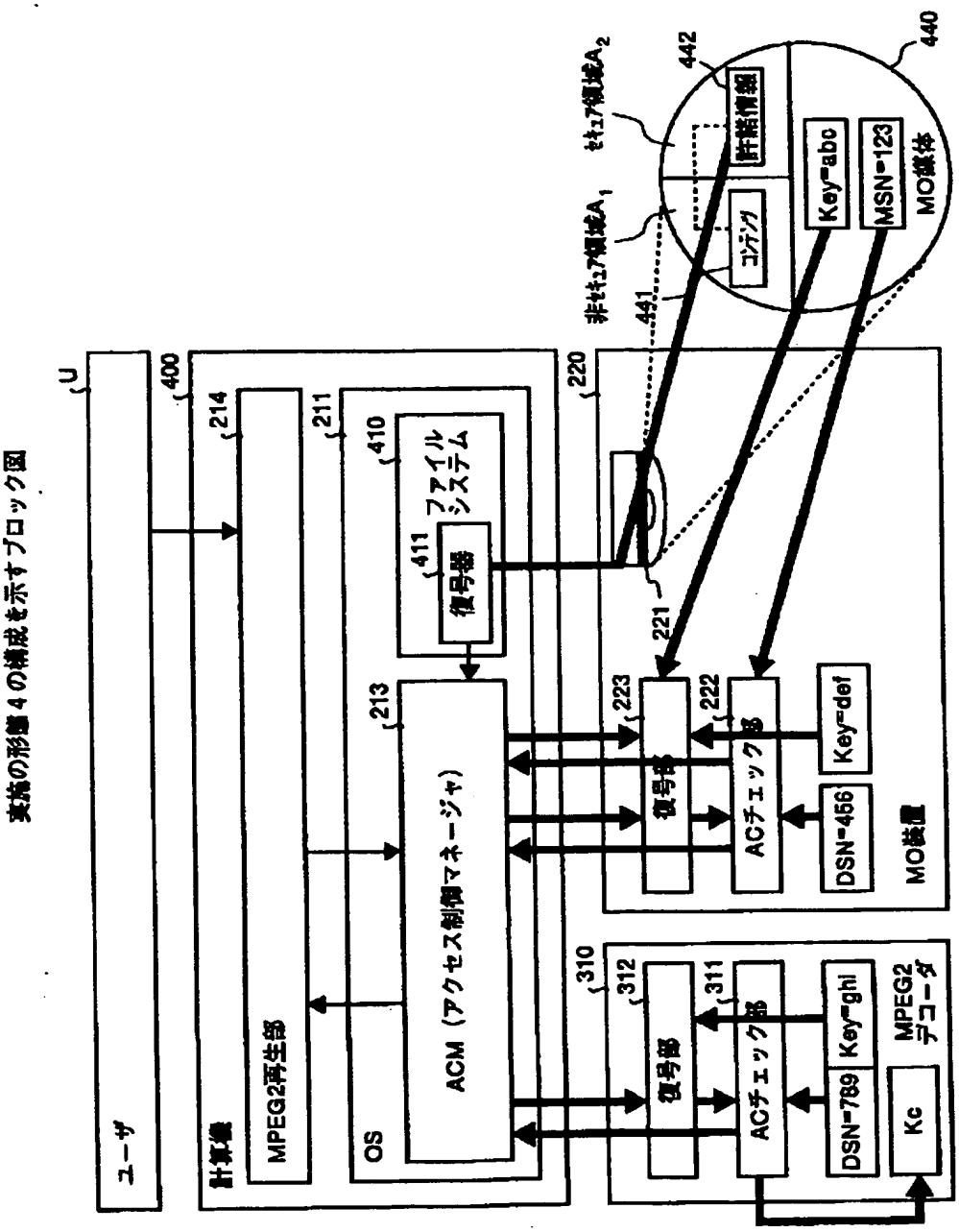
実施の形態４の動作を説明するフローチャート



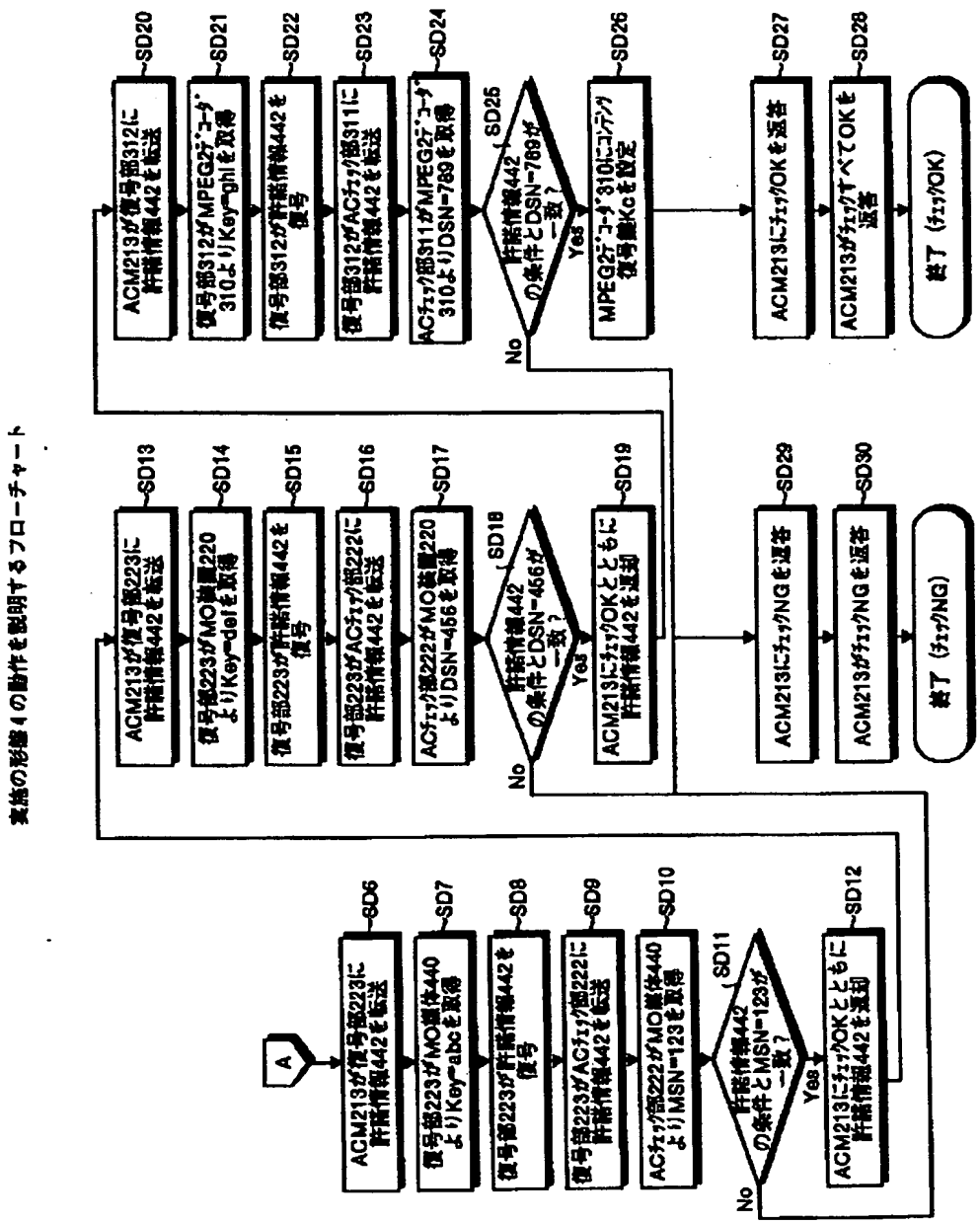
【図１３】


実施の形態３の動作を説明するフローチャート
開始
ユーザUがMPEG2の再生を指示
MPEG2再生部214がMPEG2の再生を指示
ACM213がファイルシステム212経由で許諾情報300を取得
ACM213が復号部223に許諾情報300を転送
復号部223がMO装置240よりKey-abcを取得
復号部223が許諾情報300を復号
復号部223がACチェック部222に許諾情報300を転送
ACチェック部222がMO装置240よりMSN-123を取得
SC9
許諾情報300の条件とMSN-123が一致？
No
Yes
ACM213にチェックOKとともに許諾情報300を返却
SC10
B
ACM213が復号部223に許諾情報300を転送
SC11
復号部223がMO装置220よりKey-defを取得
SC12
復号部223が許諾情報300を復号
SC13
復号部223がACチェック部221に許諾情報300を転送
SC14
ACチェック部222がMO装置220よりDSN-456を取得
SC15
許諾情報300の条件とDSN-456が一致？
SC16
No
Yes
ACM213にチェックOKとともに許諾情報300を返却
SC17
C
ACM213にチェックNGを返答
SA27
ACM213がチェックNGを返答
SA28
終了（チェックNG）
ACM213が復号部312に許諾情報300を転送
SC18
復号部312がMPEG2ｺﾝﾃﾝﾂ'310よりKey-ghiを取得
SC19
復号部312が許諾情報300を復号
SC20
復号部312がACチェック部311に許諾情報300を転送
SC21
ACチェック部311がMPEG2ｺﾝﾃﾝﾂ'310よりDSN-789を取得
SC22
許諾情報300の条件とDSN-789が一致？
SC23
No
Yes
MPEG2ｺﾝﾃﾝﾂ'310にコンテンツ復号鍵Kcを設定
SC24
ACM213にチェックOKを返答
SC25
ACM213がチェックすべてOKを返答
SC26
終了（チェックOK）

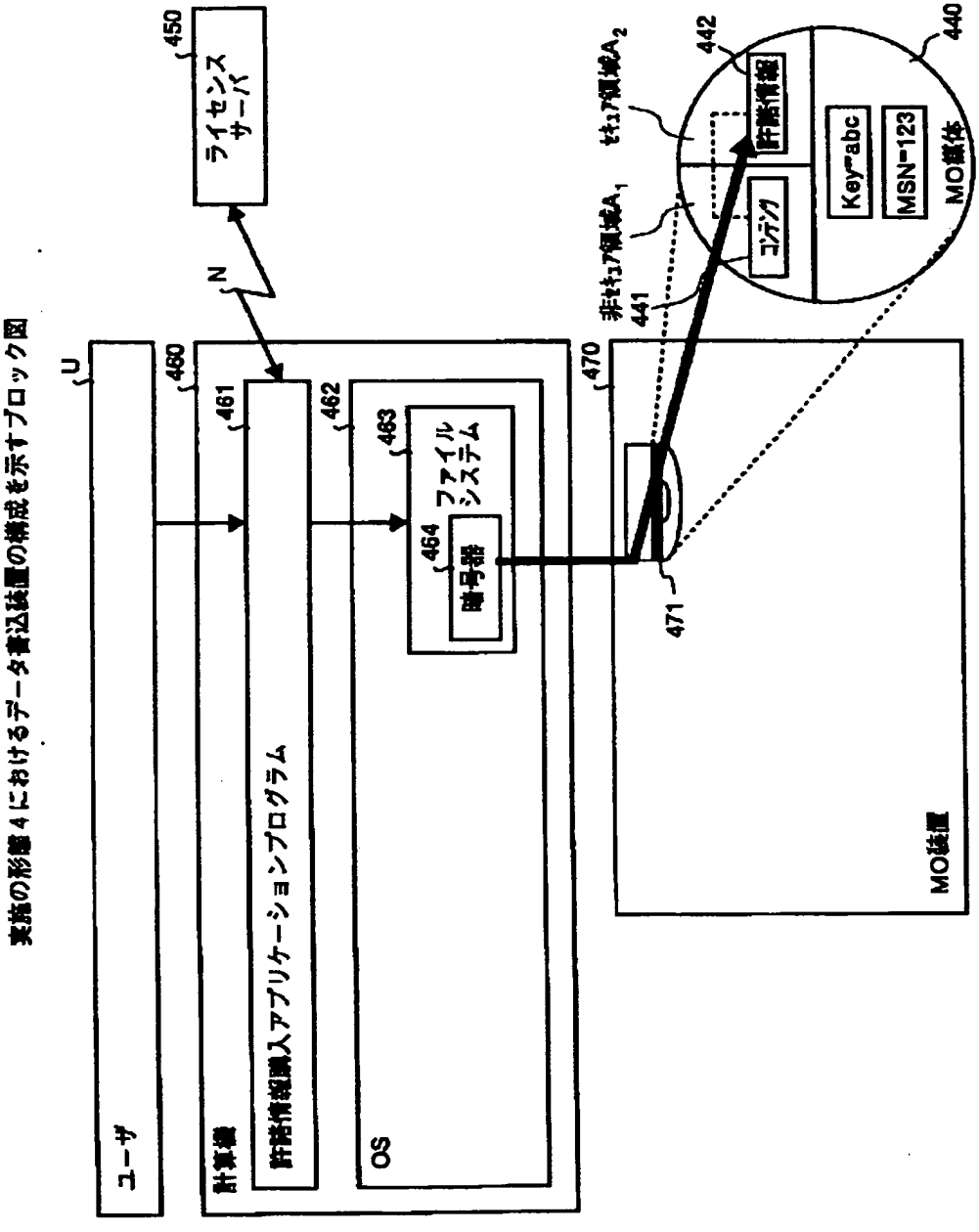
【図１４】


実施の形態４の構成を示すブロック図
U
ユーザ
400
計算機
214
MPEG2再生部
211
OS
410
ファイルシステム
411
復号器
213
ACM（アクセス制御マネージャ）
220
221
223
復号部
222
ACチェック部
Key=def
DSN=456
MO装置
310
312
復号部
311
ACチェック部
DSN=789
Key=ghi
Kc
MPEG2デコーダ
441
非セキュア領域A1
セキュア領域A2
442
許諾情報
コンテンツ
Key=abc
MSN=123
MO媒体
440

【図１７】

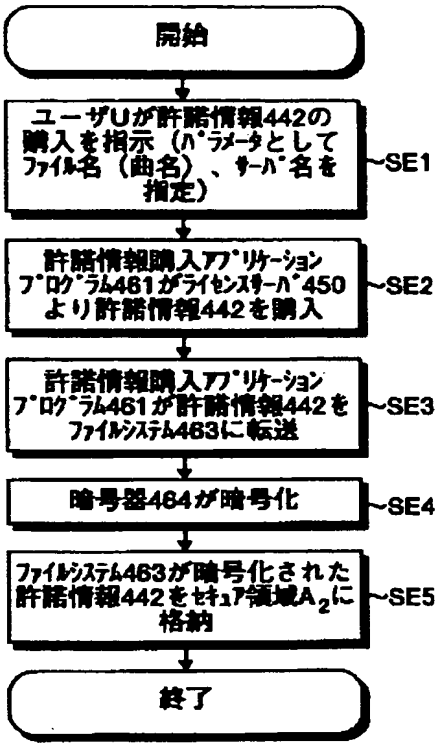

実施の形態４の動作を説明するフローチャート
A
SD6
ACM213が復号部223に許諾情報442を転送
SD7
復号部223がMO媒体440よりKey-abcを取得
SD8
復号部223が許諾情報442を復号
SD9
復号部223がACチェック部222に許諾情報442を転送
SD10
ACチェック部222がMO媒体440よりMSN-123を取得
SD11
許諾情報442の条件とMSN-123が一致？
Yes
No
SD12
ACM213にチェックOKとともに許諾情報442を返却
SD13
ACM213が復号部223に許諾情報442を転送
SD14
復号部223がMO媒体220よりKey-defを取得
SD15
復号部223が許諾情報442を復号
SD16
復号部223がACチェック部222に許諾情報442を転送
SD17
ACチェック部222がMO媒体220よりDSN-456を取得
SD18
許諾情報442の条件とDSN-456が一致？
Yes
No
SD19
ACM213にチェックOKとともに許諾情報442を返却
SD20
ACM213が復号部312に許諾情報442を転送
SD21
復号部312がMPEG2ﾃﾞｺｰﾀﾞ310よりKey-ghiを取得
SD22
復号部312が許諾情報442を復号
SD23
復号部312がACチェック部311に許諾情報442を転送
SD24
ACチェック部311がMPEG2ﾃﾞｺｰﾀﾞ310よりDSN-789を取得
SD25
許諾情報442の条件とDSN-789が一致？
Yes
No
SD26
MPEG2ﾃﾞｺｰﾀﾞ310にコンテンツ復号鍵Kcを設定
SD27
ACM213にチェックOKを返答
SD28
ACM213がチェックすべてOKを返答
終了（チェックOK）
SD29
ACM213にチェックNGを返答
SD30
ACM213がチェックNGを返答
終了（チェックNG）

【図１８】


実施の形態４におけるデータ書込装置の構成を示すブロック図
ユーザ
U
計算機
460
許諾情報購入アプリケーションプログラム
461
OS
462
ファイルシステム
463
暗号器
464
ライセンスサーバ
450
N
MO装置
470
471
MO媒体
440
許諾情報
442
Key="abc"
MSN="123"
コンテンツ
441

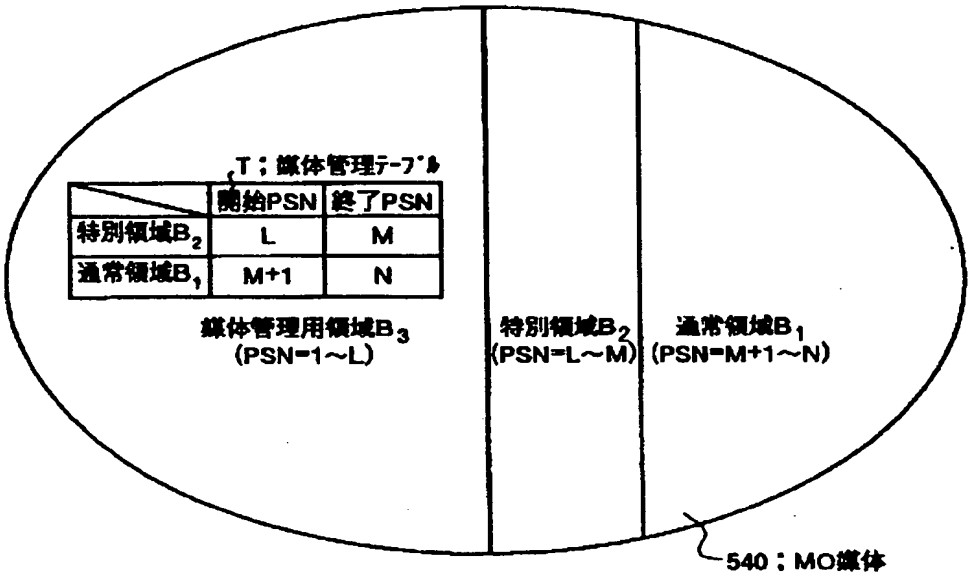
【図１９】

図18に示したデータ書込装置の動作を説明するフローチャート

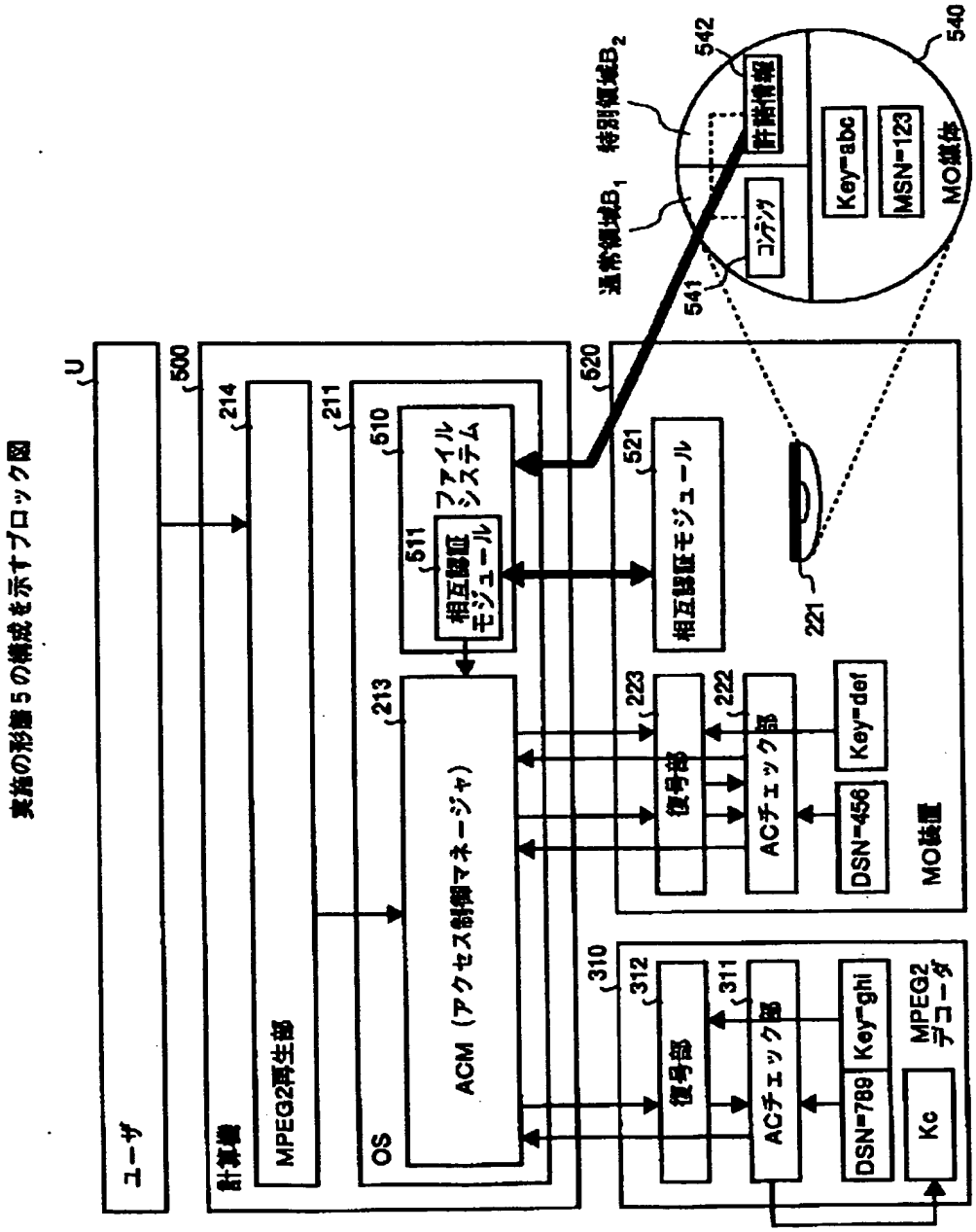


【図２１】

図20に示したMO媒体540におけるﾃﾞｰﾀ構造を示す図

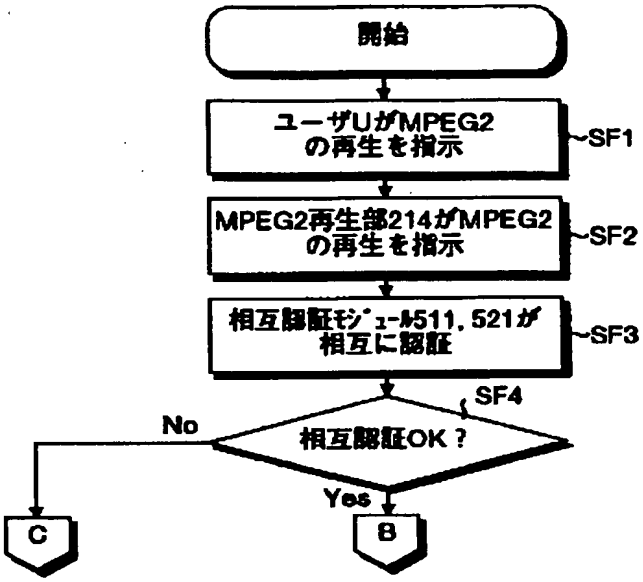


【図２０】


実施の形態５の構成を示すブロック図
U
ユーザ
500
計算機
214
MPEG2再生部
211
OS
510
ファイルシステム
511
相互認証モジュール
213
ACM（アクセス制御マネージャ）
310
312
復号部
311
ACチェック部
DSN=789
Key=ghi
Kc
MPEG2デコーダ
520
521
相互認証モジュール
223
復号部
222
ACチェック部
Key=def
DSN=456
MO装置
221
通常領域B1
特別領域B2
541
542
コンテンツ
許諾情報
Key=abc
MSN=123
MO媒体
540

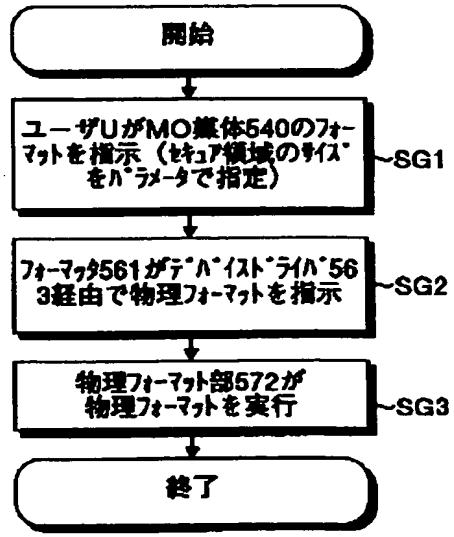
【図２２】

実施の形態５の動作を説明するフローチャート

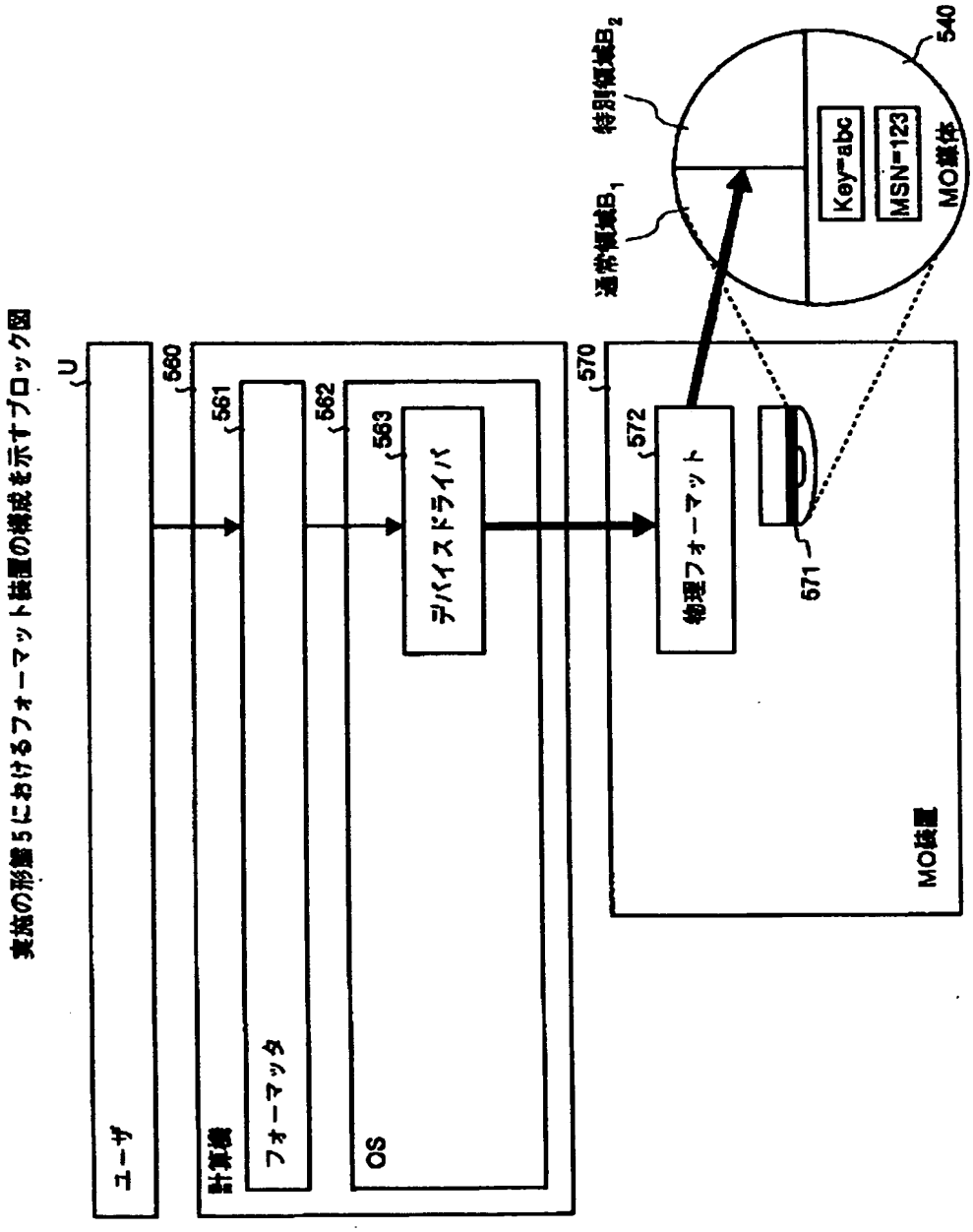


【図２４】

図23に示したフォーマット装置の動作を説明するフローチャート

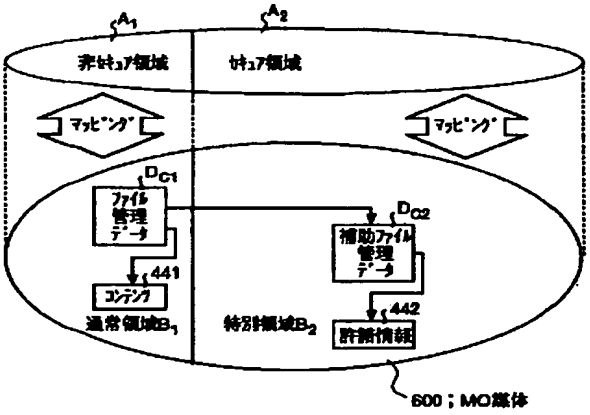


【図２３】


実施の形態5におけるフォーマット装置の構成を示すブロック図
U
ユーザ
560
計算機
561
フォーマッタ
562
OS
563
デバイスドライバ
570
MO装置
572
物理フォーマット
571
540
特別領域B2
通常領域B1
Key=abc
MSN=123
MO媒体

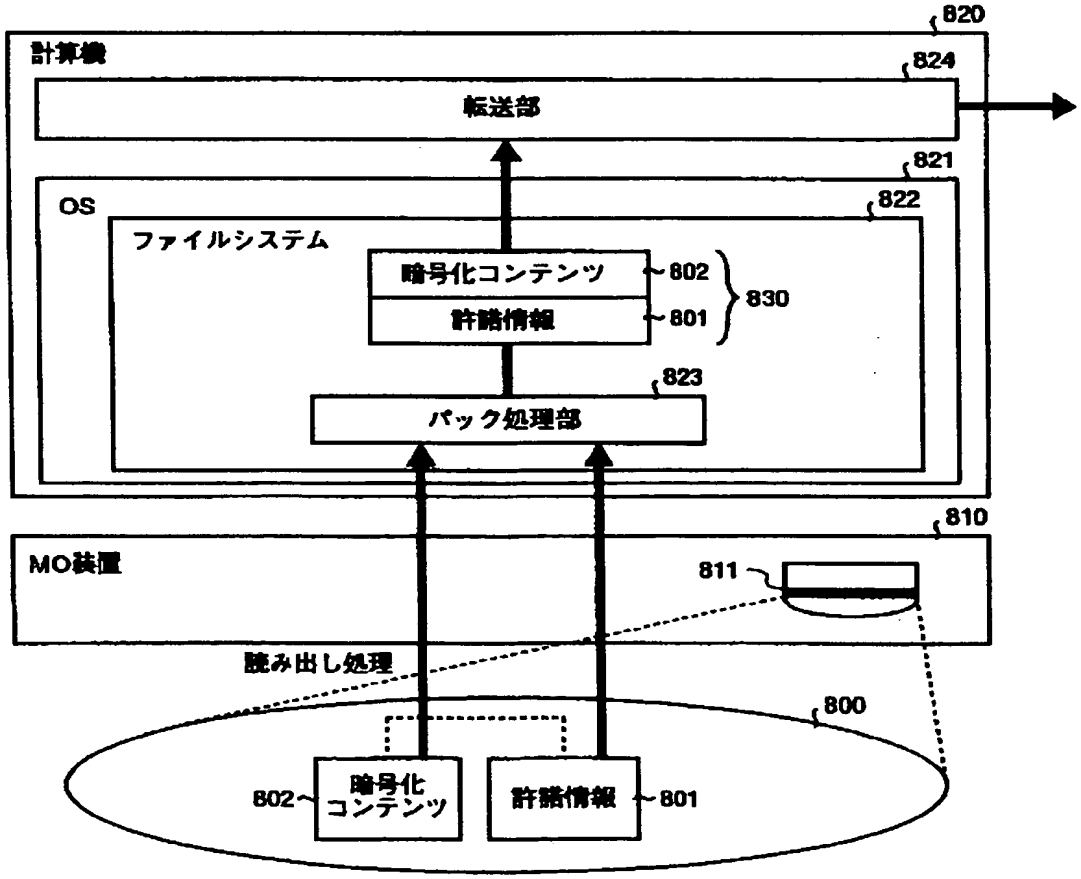
【図２５】

実施の形態６におけるMO媒体600のデータ構造を説明する図



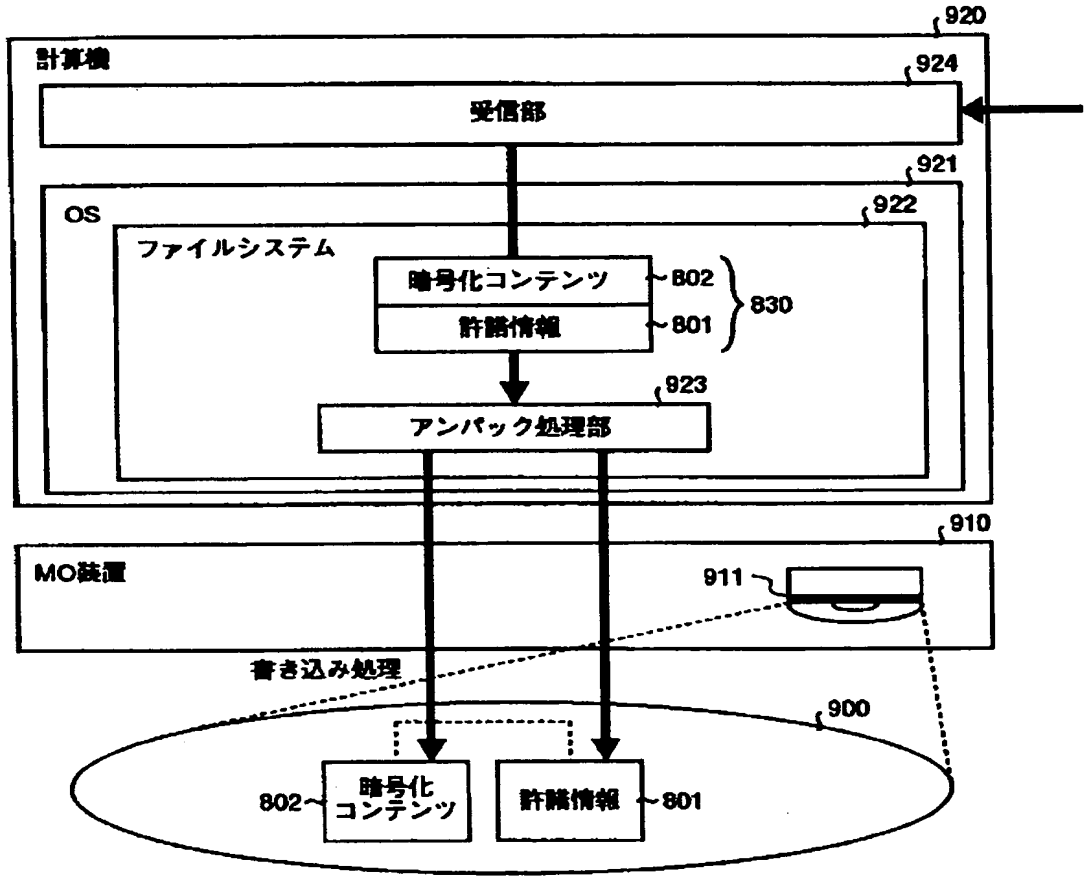
【図２６】

実施の形態７におけるパックドデータ生成装置の構成を示すブロック図



【図２７】

実施の形態７におけるアンパック装置の構成を示すブロック図



フロントページの続き

(72)発明者　小野　越夫
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　畑中　正行
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　吉田　正敏
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　中井　孝博
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5B017 AA07 BA05 BA07 BB02 BB10
CA09 CA15 CA16
5B049 AA01 AA05 BB11 CC05 EE05
EE28 GG04 GG07 GG10
5B089 GA21 JA33 JB24 KA17 KB13
KC58 KH30
9A001 EE03 LL03